Department of Economic Security
Division of Developmental Disabilities ALTCS Contract

Annual Financial Report

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Auditor General is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Bob Worsley**, Chair

Senator **Sean Bowie**

Senator **Judy Burges**

Senator **Lupe Contreras**

Senator **John Kavanagh**

Senator **Steve Yarbrough** (ex officio)

Representative **Anthony Kern**, Vice Chair

Representative **John Allen**

Representative **Rusty Bowers**

Representative **Rebecca Rios**

Representative **Athena Salman**

Representative **J.D. Mesnard** (ex officio)

Audit Staff

Jay Zsorey, Director

Victoria Fisher, Manager and Contact Person

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

ANNUAL FINANCIAL REPORT

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report

Members of the Arizona State Legislature

Michael Trailor, Director
Department of Economic Security

Report on the financial statements

We have audited the accompanying financial statements of the State of Arizona, Department of Economic Security, Division of Developmental Disabilities, Arizona Long Term Care System Contract (ALTCS Contract), as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the Division's ALTCS Contract's financial statements as listed in the table of contents.

Management's responsibility for the financial statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' responsibility

Our responsibility is to express opinions on these financial statements based on our audit. We conducted our audit in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditors consider internal control relevant to the Division's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Division's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions.

Opinions

In our opinion, the financial statements referred to above present fairly, in all material respects, the respective financial position of the Division's ALTCS Contract as of June 30, 2017, and the respective changes in financial position thereof for the year then ended in accordance with U.S. generally accepted accounting principles.

Emphasis of matter

As described in Note 1 to the financial statements, the Division's ALTCS Contract's financial statements are intended to present the financial position and the changes in financial position of only that portion of the governmental activities and major fund of the State of Arizona that is attributable to the Division's ALTCS Contract's transactions. They do not purport to, and do not, present fairly the financial position of the State of Arizona as of June 30, 2017, and the changes in its financial position for the year then ended in conformity with U.S. generally accepted accounting principles. Our opinion is not modified with respect to this matter.

Other matters

Supplementary information

Our audit was conducted for the purpose of forming opinions on the financial statements that collectively comprise the Division's ALTCS Contract's financial statements. The supplementary schedules listed in the table of contents are presented for purposes of additional analysis and are not required parts of the financial statements.

The supplementary schedules are management's responsibility and were derived from and relate directly to the underlying accounting and other records used to prepare the financial statements. Such information has been subjected to the auditing procedures applied in the audit of the financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and other additional procedures in accordance with U.S. generally accepted auditing standards. In our opinion, the supplementary schedules are fairly stated, in all material respects, in relation to the financial statements as a whole.

Other reporting required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we have also issued our report dated November 21, 2017, on our consideration of the Division's internal control over financial reporting and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements and other matters. The purpose of that report is solely to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the Division's internal control over financial reporting or on compliance. That report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Division's internal control over financial reporting and compliance.

Debbie Davenport
Auditor General

November 21, 2017

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Balance sheet—special revenue fund
June 30, 2017

Assets	
Cash and investments held by the State Treasurer	$ 1,501,155
Due from other state funds	113,704,182
Due from providers	2,696,893
Total assets	$ 117,902,230
Liabilities and fund balance	
Liabilities:	
Accrued administrative and payroll costs	$ 10,337,881
Accrued medical and healthcare claims	87,521,055
Due to other state funds	2,449,516
Total liabilities	100,308,452
Fund balance:	
Restricted for health and welfare	17,593,778
Total liabilities and fund balance	$ 117,902,230

See accompanying notes to financial statements.

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Statement of revenues, expenditures, and changes in fund balance—special revenue fund
Year ended June 30, 2017

Revenues:	
Capitation	$ 1,315,754,215
Investment earnings	1,263,346
Miscellaneous	1,283,125
Total revenues	1,318,300,686
Expenditures:	
Health and welfare:	
Aid to individuals	1,136,669,710
Allocated administrative expenditures	58,586,904
Case management	57,333,402
Professional and outside services	4,969,569
Premium tax	26,509,614
Total expenditures	1,284,069,199
Excess of revenues over expenditures	34,231,487
Other financing uses:	
Transfers to other state funds	(40,690,134)
Net change in fund balance	(6,458,647)
Fund balance, July 1, 2016	24,052,425
Fund balance, June 30, 2017	$ 17,593,778

See accompanying notes to financial statements.

Note 1 - Summary of significant accounting policies

The accounting policies of the Department of Economic Security (Department), Division of Developmental Disabilities (Division), Arizona Long Term Care System Contract (ALTCS Contract), conform to U.S. generally accepted accounting principles applicable to governmental units adopted by the Governmental Accounting Standards Board.

A. Reporting entity

For financial reporting purposes, the ALTCS Contract includes only that portion of the State's general fund that is attributable to the ALTCS Contract's transactions. The Division is responsible for administering the ALTCS Contract. Control by the Division was determined on the basis of accountability. Fiscal responsibility for the Division remains with the Department and, ultimately, with the State. The Division is a contractor with the Arizona Health Care Cost Containment System (AHCCCS) to provide medical and healthcare services to eligible enrollees of the AHCCCS Arizona Long Term Care System (ALTCS) program for the developmentally disabled. This program provides in-patient and out-patient medical and nursing services in addition to managed institutional and home- and community-based, long-term care services to eligible enrollees of the AHCCCS ALTCS program. The Division receives monthly premiums from AHCCCS for all eligible enrollees under the AHCCCS ALTCS program for the developmentally disabled.

B. Fund accounting

The Division's accounts are maintained in accordance with the principles of fund accounting to ensure that limitations and restrictions on the Division's available resources are observed. The principles of fund accounting require that resources be classified for accounting and reporting purposes into funds in accordance with the activities or objectives specified for those resources. Each fund is considered a separate accounting entity, and its operations are accounted for in a separate set of self-balancing accounts that comprise its assets, liabilities, fund balance, revenues, and expenditures.

The ALTCS Contract's financial transactions are reported as a special revenue fund since the proceeds are from specific revenue sources that are legally restricted to expenditures for specified purposes.

Although the ALTCS Contract is considered a special revenue fund when reported on individually, it becomes a part of the State's general fund at the combined state-wide level.

C. Basis of accounting

The ALTCS Contract financial statements are reported using the current financial resources measurement focus and the modified accrual basis of accounting. Under this method, revenues are recognized when they become both measurable and available. Revenues are considered to be available when they are collected within the current period or soon enough thereafter to pay liabilities of the current period. For this purpose, the Division considers capitation revenues to be available if they are collected within 90 days of the end of the current fiscal year and considers all other revenues to be available if they are collected within 30 days of the end of the current fiscal year. All ALTCS Contract revenue sources are susceptible to accrual. Expenditures are recognized when the related fund liability is incurred.

D. Fund balance classifications

Fund balance is reported separately within classifications based on a hierarchy of the constraints placed on the use of those resources. The classifications are based on the relative strength of the constraints that control how the specific amounts can be spent. The classifications are nonspendable, restricted, and unrestricted, which includes committed, assigned, and unassigned fund balance classifications.

Restricted fund balances are those that have externally imposed restrictions on their usage by creditors, such as through debt covenants, grantors, contributors, or laws and regulations. Deficits in fund balance, if any, are reported as unassigned.

E. Capitation

The ALTCS Contract receives fixed capitation payments from AHCCCS based on certain rates for each AHCCCS member enrolled in the Division's ALTCS Contract program. The ALTCS Contract is required to provide all covered healthcare services to its members, regardless of the cost of care. If there are monies remaining, the ALTCS Contract retains the monies as profit; if the costs are higher than the amount of capitation payments from AHCCCS, the ALTCS Contract absorbs the loss.

F. Investment earnings

Investment earnings is composed of interest earned on the ALTCS Contract's portion of monies deposited with the State Treasurer.

G. Incurred but not reported (IBNR) methodology

The liability and expenditures reported for accrued medical and healthcare claims include IBNR medical claims, which are estimated using lag data provided by the Division's information systems, with adjustments as necessary for events that are outside the lag patterns. Amounts are based on historical expenditure patterns.

Note 2 - Cash and investments held by the State Treasurer

Arizona Revised Statutes (A.R.S.) require state agencies' monies to be deposited with the State Treasurer and further requires those deposits to be invested in various pooled funds. Cash and investments held by the State Treasurer represent the ALTCS Contract's portion of those monies. The State Treasurer invests idle contract monies in an internal investment pool (Pool 3) and distributes interest to the ALTCS Contract. Interest earned from these invested monies is allocated monthly based on the average daily balance. Participant shares in the pool are purchased and sold based on the net position value of the shares. The net position value is determined by dividing the fair value of the portfolio by the total shares of the pool outstanding. As a result, the ALTCS Contract's portion of the pool is not identified with specific investments. The ALTCS Contract's portion of these deposits and investments is reported at fair value, measured on a monthly basis, which approximates the ALTCS Contract's value of participant pool shares.

The State Treasurer's internal investment pool 3 is not required to be registered and is not registered with the Securities and Exchange Commission under the Dodd-Frank Act of 2010. The activities and performance of the pool is reviewed monthly by the State Board of Investment in accordance with A.R.S. §35-311.

At June 30, 2017, the ALTCS Contract's deposits with the State Treasurer were as follows:

	Amount
State Treasurer's investment pool 3	$1,501,155

Credit Risk—Credit risk is the risk that an issuer or counterparty to an investment will not fulfill its obligations. The Department of Economic Security does not have a formal investment policy with respect to credit risk. The State Treasurer's investment pool 3 is unrated.

Interest Rate Risk—Interest rate risk is the risk that changes in interest rates will adversely affect the fair value of an investment. The Department of Economic Security does not have a formal interest rate risk policy. As of June 30, 2017, the State Treasurer's weighted average to maturity of its internal pool 3 investments is 1.70 years.

Note 3 - Due from other state funds

Amounts due from other state funds at June 30, 2017, include:

- $112,913,399 of capitation and reinsurance,
- $292,625 of interest earned, and
- $498,158 of share of costs and miscellaneous.

Note 4 - Due from providers

The amount due from providers at June 30, 2017, is $2,696,893 as a result of post-payment reviews of long-term care home- and community-based service providers.

Note 5 - Accrued medical and healthcare claims

Accrued medical and healthcare claims totaling $87,521,055, include $83,302,348 of IBNR medical claims and a special accrual of $4,218,707 for events that are outside the payment lag patterns.

Note 6 - Due to other state funds

Amounts due to other state funds at June 30, 2017, include:

- $2,182,704 of premium tax payable to the Arizona Department of Insurance and
- $266,812 of assessments payable to the state general fund.

Note 7 - Acute care reinsurance

During the year ended June 30, 2017, the Division received reimbursements totaling $7,767,556 from AHCCCS for acute care reinsurance expenditures for claims for enrollees incurred in the current and prior fiscal years. These reimbursements are recorded as a reduction of aid to individuals expenditures.

The Division subcontracts with various health plans to provide acute care services to ALTCS enrollees. These health plans must submit clean reinsurance claims to the Division within 15 months from the date of service.

The Division disbursed a total of $10,149,399 to health plans during the year ended June 30, 2017.

Note 8 - Aid to individuals expenditures

Aid to individuals expenditures consists of expenditures summarized by type of service setting or service provided, as applicable:

Institutional care:	
Skilled nursing	$ 4,584,884
Institutional care	14,389,263
Intermediate (intellectually or developmentally disabled)	10,879,365
Institutional care IBNR	2,689,230
Total institutional care	32,542,742
Home- and community-based services (HCBS):	
State-operated group home	5,647,516
Vendor-operated group home	289,834,810
Adult developmental home	59,944,916
Home-based services	492,281,030
HCBS IBNR	82,912,404
Total HCBS	930,620,676
Acute care:	
Acute care	169,205,028
Acute care IBNR	1,919,421
Reinsurance	10,149,399
Reinsurance reimbursement	(7,767,556)
Total acute care	173,506,292
Total aid to individuals expenditures	$1,136,669,710

During the year ended June 30, 2017, the ALTCS Contract recorded allocated charges of $21,561,078 as expenditures for direct care services, including administrative costs the Division provided to clients. The expenditures were charged to the ALTCS Contract as aid to individuals expenditures based on a federally approved cost allocation plan.

Note 9 - Allocated administrative expenditures

During the year ended June 30, 2017, the ALTCS Contract recorded allocated administrative charges of $58,586,904 as expenditures for its share of the administrative and fiscal services the Department provided.

Note 10 - Premium tax

Arizona Revised Statutes §§36-2905 and 36-2944.01 require the ALTCS Contract to pay a 2 percent premium tax on all capitation and other reimbursements received. These premium taxes are reported as expenditures and are paid to the Arizona Department of Insurance.

Note 11 - Transfers

Transfers to other state funds during the year ended June 30, 2017, consisted of $24,052,425 to the State General Fund and $2,144,309 to the state-funded long-term care fund as a result of Laws 2017, First Regular Session, Chapter 305, Section 139, that amended A.R.S. §36-2953 and $14,493,400 to the state-funded long-term care fund as a result of Laws 2017, First Regular Session, Chapter 309, Section 18.

Note 12 - Commitments and contingencies

The State has the ultimate fiscal responsibility for the ALTCS Contract. Accordingly, any claims requiring additional resources require the Legislature's approval. Although there is a possibility that claims could be asserted that would require additional resources for the ALTCS Contract, in the division management's opinion, the possibility is low that valid claims will be asserted and claim amounts cannot reasonably be estimated.

Note 13 - Risk management

The Division is exposed to various risks of loss related to torts; theft of, damage to, and destruction of assets; errors and omissions; injuries to employees; medical malpractice; and natural disasters. The Department is a participant in the State's self-insurance program, and in the division management's opinion, any unfavorable outcomes from these risks would be covered by that self-insurance program. Accordingly, the Department has no risk of loss beyond adjustments to future years' premium payments to the State's self-insurance program. All estimated losses for the State's unsettled claims and actions are determined on an actuarial basis and are included in the *State of Arizona Comprehensive Annual Financial Report*.

Note 14 – Related-party transactions

During the year ended June 30, 2017, the ALTCS Contract reimbursed the Division for $21,561,078 of health and rehabilitative services provided to enrollees, including administrative costs. The ALTCS Contract also reimbursed the Division as well as other department divisions for $58,586,904 of administrative and fiscal services and the Arizona Department of Insurance for $26,509,614 of premium taxes.

This page is intentionally left blank.

Supplementary schedules

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Lag report for institutional care payments
Year Ended June 30, 2017

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 6,179,928	$ 2,151,398	$ 63,914	$ 14,520				$ 8,409,760
1st Prior		6,302,347	2,056,865	34,267	$ 6,950			8,400,429
2nd Prior			5,882,133	1,717,155	51,125	$ 31,900	$ 26,326	7,708,639
3rd Prior				6,519,804	171,927	58,569	7,751	6,758,051
4th Prior					6,322,274	1,546,857	37,904	7,907,035
5th Prior						6,191,584	1,552,350	7,743,934
6th Prior							5,884,490	5,884,490
Total	6,179,928	8,453,745	8,002,912	8,285,746	6,552,276	7,828,910	7,508,821	52,812,338
Expenses reported	8,574,217	8,643,883	7,956,821	7,367,821	8,586,389	7,312,867	7,757,027	56,199,025
Adjustment (1)	(226,741)	258,475	97,533	939,222	(2,033,783)	516,043	(248,206)	(697,457)
Remaining liability	$ 2,167,548	$ 448,613	$ 51,442	$ 21,297	$ 330	$ -	$ -	$ 2,689,230

(1) Adjustment amounts each quarter fluctuate because of unpredictable variables that affect the business cycle.

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Lag report for home- and community-based services payments
Year Ended June 30, 2017

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 163,371,297	$ 85,439,658	$ 944,571	$ 495,563	$ 330,620	$ (46,164)	$ 719	$ 250,536,264
1st Prior		151,010,185	72,571,679	1,228,860	347,349	360,077	(576)	225,517,574
2nd Prior			147,832,948	72,747,155	1,119,378	390,470	88,052	222,178,003
3rd Prior				148,854,633	75,108,275	1,229,060	396,291	225,588,259
4th Prior					140,049,175	71,102,025	969,280	212,120,480
5th Prior						134,421,735	70,260,457	204,682,192
6th Prior							137,908,224	137,908,224
Total	163,371,297	236,449,843	221,349,198	223,326,211	216,954,797	207,457,203	209,622,447	1,478,530,996
Expenses reported	243,526,402	231,331,456	228,569,857	227,192,961	216,076,777	207,215,255	213,139,553	1,567,052,261
Adjustment (1)	(2,623,891)	7,283,776	(5,322,059)	(2,549,685)	878,156	241,948	(3,517,106)	(5,608,861)
Remaining liability	$ 77,531,214	$ 2,165,389	$ 1,898,600	$ 1,317,065	$ 136	$ -	$ -	$ 82,912,404

(1) Adjustment amounts each quarter fluctuate because of unpredictable variables that affect the business cycle.

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Lag report for acute care payments
Year Ended June 30, 2017

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 40,214,626	$ 817,779	$ 760,267	$ 414,767	$ 788,584	$ 10,161	$ 7,140	$ 43,013,324
1st Prior		45,069,107	976,311	747,132	75,259	43,048	19,463	46,930,320
2nd Prior			40,043,060	856,246	356,797	114,193	62,332	41,432,628
3rd Prior				39,770,986	1,169,035	463,767	637,390	42,041,178
4th Prior					33,598,255	757,177	1,195,003	35,550,435
5th Prior						38,330,782	1,146,020	39,476,802
6th Prior							33,923,254	33,923,254
Total	40,214,626	45,886,886	41,779,638	41,789,131	35,987,930	39,719,128	36,990,602	282,367,941
Expenses reported (2)	47,650,515	47,495,189	42,617,968	43,510,176	42,939,633	40,776,358	35,489,783	300,479,622
Adjustment (1)	(6,455,808)	(930,700)	(612,787)	(1,693,899)	(6,944,722)	(1,055,163)	1,500,819	(16,192,260)
Remaining liability	$ 980,081	$ 677,603	$ 225,543	$ 27,146	$ 6,981	$ 2,067	$ -	$ 1,919,421

(1) Adjustment amounts each quarter fluctuate because of unpredictable variables that affect the business cycle.
(2) Acute Care Payments include fee for service, capitation, and reinsurance payments. Reinsurance reimbursements are not included.

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Related-party transactions
Year Ended June 30, 2017

Related party and relationship	Service provided	Description of transactions or payment terms agreement	Amount
Department of Economic Security, Division of Developmental Disabilities, Intermediate Care Facility/Mentally Retarded, State Facilities	Health and rehabilitative services and administrative costs	Allocated by Title XIX case management time reporting, member days count, and modified total direct costs	$10,879,366
Department of Economic Security, Division of Developmental Disabilities, State-Operated Group Homes, Home-Based Services, State Facilities	Health and rehabilitative services and administrative costs	Allocated by Title XIX case management time reporting, member days count, and modified total direct costs	10,681,712
Department of Economic Security, Division of Developmental Disabilities and all other divisions	Administrative and fiscal services	Allocated departmental overhead costs	58,586,904
Department of Insurance	Compliance with A.R.S. §§36-2905 and 36-2944.01	Premium tax payments	26,509,614

This page is intentionally left blank.

INTERNAL CONTROL/COMPLIANCE REPORT

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

Michael Trailor, Director
Department of Economic Security

We have audited, in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, the financial statements of the State of Arizona, Department of Economic Security, Division of Development Disabilities, Arizona Long Term Care System Contract (ALTCS Contract), as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the Division's ALTCS Contract's financial statements, and have issued our report thereon dated November 21, 2017.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the Division's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the Division's ALTCS Contract's financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Division's internal control. Accordingly, we do not express an opinion on the effectiveness of the Division's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying schedule of findings and recommendations, we identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the Division's ALTCS Contract's financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiency described in the accompanying schedule of findings and recommendations as item 2017-01 to be a material weakness.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying schedule of findings and recommendations as items 2017-02, 2017-03, 2017-04, and 2017-05 to be significant deficiencies.

Compliance and other matters

As part of obtaining reasonable assurance about whether the Division's ALTCS Contract's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Division of Development Disabilities response to findings

The Division of Development Disabilities' responses to the findings identified in our audit are presented in its corrective action plan at the end of this report. The Division's responses were not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the Division's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Division's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Debbie Davenport
Auditor General

November 21, 2017

Financial statement findings

2017-01

The Department of Economic Security should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect the Department of Economic Security's (Department) information technology (IT) resources, which include its systems, network, infrastructure, and data, from unauthorized or inappropriate access or use, manipulation, damage, or loss. Logical access controls also help to ensure that authenticated users access only what they are authorized to. Therefore, the Department should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The Department has written policies for managing access to its IT resources; however, the Department lacks adequate procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

Effect—There is an increased risk that the Department may not prevent or detect unauthorized or inappropriate access or use, manipulation, damage, or loss of its IT resources, including sensitive and confidential information.

Cause—Various divisions operate the Department's IT systems, and the Department is working on its multiyear corrective action plan to remediate the deficiencies noted in a prior year.

Recommendation—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the Department needs to develop effective logical and physical access procedures over its IT resources. The Department should review these procedures against current IT standards and best practices and implement them department-wide, as appropriate. Further the Department should train staff on the procedures. The information below provides guidance and best practices to help the Department achieve this objective.

- **Review user access**—A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities. Also, when an employee's job responsibilities change, a review of their access should be performed to ensure their access is compatible with their new job responsibilities.
- **Remove terminated employees' access to its IT resources**—Employees' network and system access should immediately be removed upon their terminations.
- **Review contractor and other nonentity account access**—A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.

- **Review all shared accounts**—Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts**—Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users**—Key activities of users and those with elevated access should be reviewed for propriety.
- **Manage employee-owned and entity-owned electronic devices connecting to the network**—The use of employee-owned and entity-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to network.
- **Manage remote access**—Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data center access**—A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed.

The Department's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

This finding is similar to prior-year finding 2016-02.

2017-02

The Department of Economic Security should improve its risk-assessment process to include information technology security

Criteria—The Department of Economic Security (Department) faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include an entity-wide risk-assessment process that involves members of the Department's administration and IT management to determine the risks the Department faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances; and identifying, analyzing, and responding to identified risks.

Condition and context—The Department's annual risk-assessment process did not include a department-wide information technology (IT) security risk assessment over the Department's IT resources, which include its systems, network, infrastructure, and data. Also, the Department did not identify and classify sensitive information. Further, the Department did not evaluate the impact disasters or other system interruptions could have on its critical IT resources.

Effect—There is an increased risk that the Department's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The Department is working on its multiyear corrective action plan to remediate the deficiencies noted in a prior year.

Recommendations—To help ensure the Department has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the Department needs to implement a department-wide IT risk-assessment process. The information below provides guidance and best practices to help the Department achieve this objective.

- **Conduct an IT risk-assessment process at least annually—**A risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of an entity's security vulnerability scans.
- **Identify, classify, inventory, and protect sensitive information—**Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.
- **Evaluate the impact disasters or other system interruptions could have on critical IT resources—**The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

The Department's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

2017-03

The Department of Economic Security should improve their configuration management processes over their information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that the Department of Economic Security's (Department) information technology (IT) resources, which include its systems, network, infrastructure, and data, are configured securely and that changes to these IT resources do not adversely affect security or operations. IT resources are typically constantly changing in response to new, enhanced, corrected, or updated hardware and software capabilities and new security threats. The Department should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—The Department has written policies for configuration management; however, the Department lacks written procedures for managing changes to its IT resources and ensuring IT resources were configured securely.

Effect—There is an increased risk that the Department's IT resources may not be configured appropriately and securely and that changes to those resources could be unauthorized or inappropriate or could have unintended results without proper documentation, authorization, review, testing, and approval prior to being applied.

Cause—The Department is still working on its multiyear corrective action plan to remediate the deficiencies noted in a prior year.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the Department needs to develop configuration management procedures. The Department should review these procedures against current IT standards and best practices and implement them department-wide, as appropriate. Further, the Department should train staff on the procedures. The information below provides guidance and best practices to help the Department achieve this objective.

- **Roll back changes—**Roll back procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Maintain configuration settings—**Maintain appropriate and secure configurations for all systems.
- **Manage software installed on employee computer workstations—**For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

The Department's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

This finding is similar to prior-year finding 2016-03.

2017-04

The Department of Economic Security should improve security over their information technology resources

Criteria—The selection and implementation of security controls for the Department of Economic Security's (Department) information technology (IT) resources, which include its systems, network, infrastructure, and data, are important because they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the Department's operations or assets. Therefore, the Department should implement internal control policies and procedures for an effective IT security process that includes practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

Condition and context—The Department has written security policies over its IT resources; however, it lacked sufficient written security procedures.

Effect—There is an increased risk that the Department may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—The Department is working on its multiyear corrective action plan to remediate the deficiencies noted in a prior year.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the Department needs to further develop its IT security procedures. The Department should review these procedures against current IT standards and best practices and implement them department-wide, as appropriate. Further, the Department should train staff on the policies and procedures. The information below provides guidance and best practices to help the Department achieve this objective.

- **Perform proactive logging and log monitoring—**Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents, such as unauthorized or inappropriate access. An entity should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.
- **Prepare and implement an incident response plan—**An incident response plan should be developed, tested, and implemented for an entity's IT resources, and staff responsible for the plan should be trained. The plan should coordinate incident-handling activities with contingency-planning activities and incorporate lessons learned from ongoing incident handling in the incident response procedures. The incident response plan should be distributed to incident response personnel and updated as necessary. Security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks—**A plan should be developed to provide continuous training on IT security risks, including a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats employees generate. Security awareness training should be provided to new employees and on an on-going basis.
- **Perform IT vulnerability scans—**A formal process should be developed for vulnerability scans that includes performing vulnerability scans of its IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Secure unsupported software—**Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Develop and document a process for awarding IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Further, for cloud services, ensure service contracts address all necessary security requirements based on best practices, such as physical location of data centers. Finally, an IT vendor's performance should be monitored to ensure conformance with vendor contracts.

The Department's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

This finding is similar to prior-year finding 2016-05.

2017-05

The Department of Economic Security should improve their contingency planning procedures for their information technology resources

Criteria—It is critical that the Department of Economic Security (Department) have contingency planning procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which include its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption. Contingency planning procedures include having a comprehensive, up-to-date contingency plan; taking steps to facilitate activation of the plan; and having system and data backup policies and procedures.

Condition and context—The Department's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources and did not include all systems. Also, although the Department was performing system and data backups, it did not have documented policies and procedures for performing the backups or testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The Department risks not being able to provide for the continuity of operations, recover vital IT systems and data, and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system and data recovery.

Cause—The Department is working on its multiyear corrective action plan to remediate the deficiencies noted in a prior year.

Recommendations—To help ensure department operations continue in the event of a disaster, system or equipment failure, or other interruption, the Department needs to further develop its contingency planning procedures. The Department should review its contingency planning procedures against current IT standards and best practices and implement them department-wide, as appropriate. The information below provides guidance and best practices to help the Department achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—**Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including recovery objectives and restoration priorities and metrics as determined in the entity's business-impact analysis; contingency roles and responsibilities and assigned individuals with contact information; identification of critical information assets and processes for migrating to the alternative processing site; processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered; and review and approval by appropriate personnel. The contingency plan should also be coordinated with incident-handling activities and stored in a secure location, accessible to those who need to use it, and protected from unauthorized disclosure or modification.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions, including putting contracts in place or equipping the alternative site to resume essential business functions, if necessary. The alternative site's information security safeguards should be equivalent to the primary site.

- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or table top discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.
- **Train staff responsible for implementing the contingency plan—**An ongoing training schedule should be developed for staff responsible for implementing the plan that is specific to each user's assigned role and responsibilities.
- **Backup systems and data—**Establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed. Policies and procedures should require system software and data backups to be protected and stored in an alternative site with security equivalent to the primary storage site. Backups should include user-level information, system-level information, and system documentation, including security-related documentation. In addition, critical information system software and security-related information should be stored at an alternative site or in a fire-rated container.

The Department's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

This is similar to prior-year finding 2016-04.

This page is intentionally left blank.

DIVISION RESPONSE

DEPARTMENT OF ECONOMIC SECURITY
Your Partner For A Stronger Arizona

Douglas A. Ducey
Governor

Michael Trailor
Director

November 21, 2017

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have prepared the accompanying corrective action plan as required by the standards applicable to financial audits contained in *Government Auditing Standards*. Specifically, for each finding we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Sherri Wince
Interim Deputy Assistant Director

Department of Economic Security
Corrective Action Plan
Fiscal Year 2017

FINANCIAL STATEMENT FINDINGS

2017-01
The Department of Economic Security should improve access controls over its information technology resources.
Contact: John Bautista, johnbautista@azdes.gov, (602) 774-8809.
Anticipated completion date: March 31, 2018.
Agency response: Concur

The Department has developed a detailed corrective action plan to address this finding and is aggressively working to correct all issues related to access controls over its IT resources. During the last several months, the Department has implemented all required policies and procedures and completed a significant portion of its action plan and expects to fully implement the plan by March 31, 2018.

2017-02
The Department of Economic Security should improve its risk-assessment process to include information technology security.
Contact: John Bautista, johnbautista@azdes.gov, (602) 774-8809.
Anticipated completion date: May 30, 2018.
Agency response: Concur

The Department has developed a detailed corrective action plan to address this finding and is aggressively working to correct all issues related to improving its IT risk assessment process. During the last several months the Department has implemented all required policies and procedures and completed a significant portion of its action plan and expects to fully implement the plan by May 30, 2018.

2017-03
The Department of Economic Security should improve their configuration management processes over their information technology resources.

Contact: John Bautista, johnbautista@azdes.gov, (602) 774-8809.
Anticipated completion date: December 1, 2017.
Agency response: Concur

The Department has developed a detailed corrective action plan to address this finding and is aggressively working to correct all issues related to improving its IT configuration management process. During the last several months the Department has implemented nearly all required policies and procedures and completed most of its action plan and expects to fully implement the plan by December 1, 2017.

Department of Economic Security
Corrective Action Plan
Fiscal Year 2017

2017-04
The Department of Economic Security should improve security over their information technology resources.

Contact: John Bautista, johnbautista@azdes.gov, (602) 774-8809.
Anticipated completion date: December 31, 2017.
Agency response: Concur

The Department has developed a detailed corrective action plan to address this finding and is aggressively working to correct all issues related to improving the security of its IT resources. During the last several months the Department has implemented nearly all required policies and procedures and completed most of its action plan and expects to fully implement the plan by December 31, 2017.

2017-05
The Department of Economic Security should improve their contingency planning procedures for their information technology resources.

Contact: John Bautista, johnbautista@azdes.gov, (602) 774-8809.
Anticipated completion date: July 1, 2018.
Agency response: Concur

The Department has developed a detailed corrective action plan to address this finding and is aggressively working to correct all issues related to its IT contingency planning process. During the last several months the Department has implemented all required policies and procedures and completed a significant portion of its action plan and expects to fully implement the plan by July 1, 2018.


ARIZONA
Auditor General
Making a Positive Difference