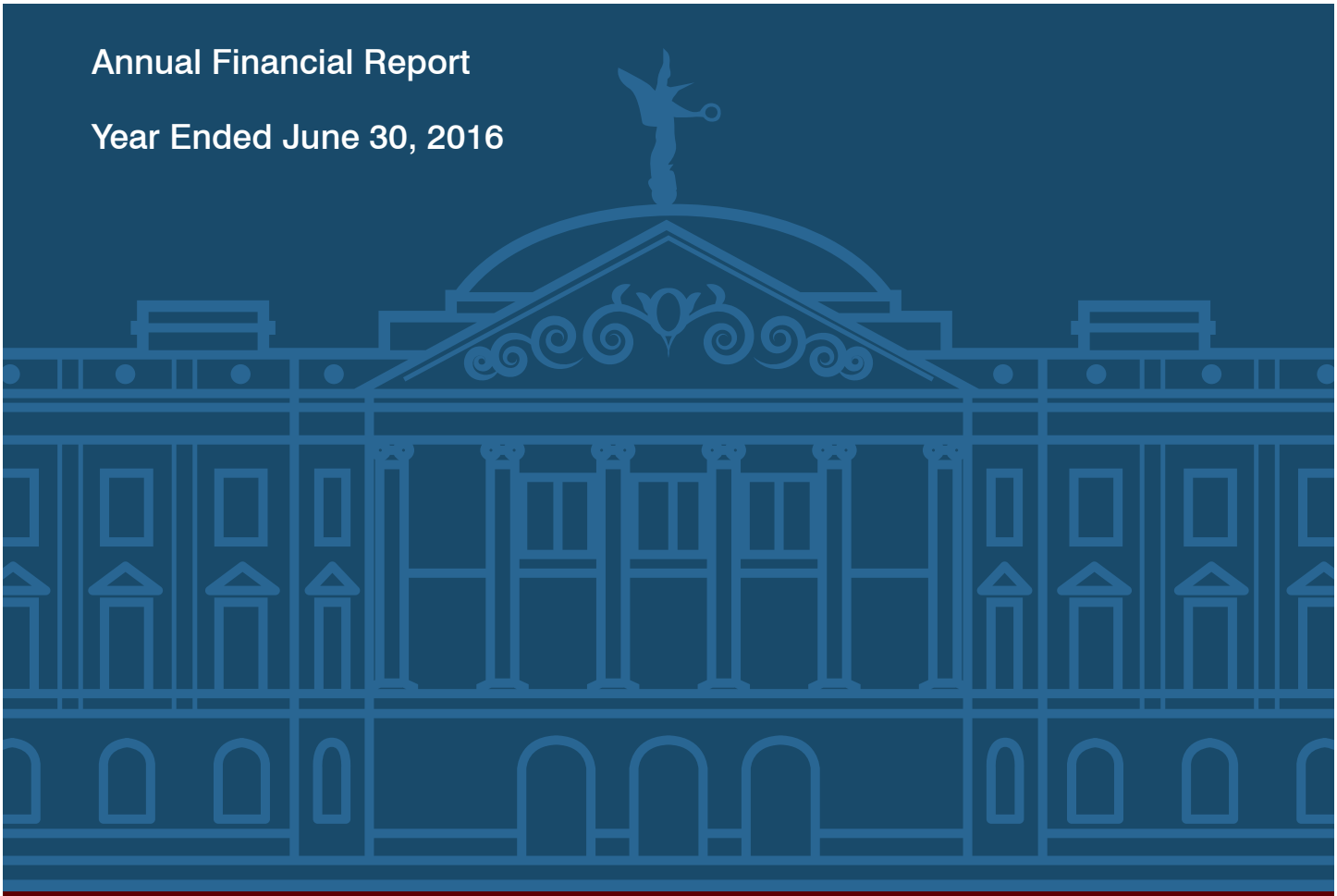
Department of Economic Security
Division of Developmental Disabilities ALTCS Contract

Annual Financial Report

Year Ended June 30, 2016



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

Representative **John Allen**, Chair
Representative **Regina Cobb**
Representative **Debbie McCune Davis**
Representative **Rebecca Rios**
Representative **Kelly Townsend**
Representative **David Gowan** (ex officio)

Senator **Judy Burges**, Vice Chair
Senator **Nancy Barto**
Senator **Lupe Contreras**
Senator **David Farnsworth**
Senator **Lynne Pancrazi**
Senator **Andy Biggs** (ex officio)

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

Timothy Jeffries, 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, 2016, 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.

Opinion

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, 2016, 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 discussed in Note 1, 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 transactions of the Division's ALTCS Contract. They do not purport to, and do not, present fairly the financial position of the State of Arizona as of June 30, 2016, 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 22, 2016, 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 other matters. The purpose of that report is 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 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 22, 2016

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Balance sheet—special revenue fund
June 30, 2016

Assets	
Cash and investments held by the State Treasurer	$ 54,324,039
Due from other state funds	103,038,676
Due from providers	2,162,197
Total assets	$ 159,524,912
Liabilities and fund balance	
Liabilities:	
Accrued administrative and payroll costs	$ 10,781,389
Accrued medical and healthcare claims	81,781,277
Due to other state funds	42,909,821
Total liabilities	135,472,487
Fund balance:	
Restricted for health and welfare	24,052,425
Total liabilities and fund balance	$ 159,524,912

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
June 30, 2016

Revenues:	
Capitation	$ 1,197,343,106
Investment earnings	3,599,233
Miscellaneous	385,489
Total revenues	1,201,327,828
Expenditures:	
Health and welfare:	
Aid to individuals	1,027,133,958
Allocated administrative expenditures	54,906,350
Case management	55,588,258
Professional and outside services	8,365,236
Premium tax	29,281,601
Total expenditures	1,175,275,403
Excess of revenues over expenditures	26,052,425
Other financing uses:	
Transfers to other state funds	(36,814,703)
Net change in fund balance	(10,762,278)
Fund balance, July 1, 2015	34,814,703
Fund balance, June 30, 2016	$ 24,052,425

See accompanying notes to financial statements.

Department of Economic Security
Division of Developmental Disabilities ALTCS Contract
Notes to financial statements
June 30, 2016

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.) requires 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. 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 1940 Investment Advisors Act. The activities and performance of the pool is reviewed monthly by the State Board of Investments in accordance with A.R.S. §35-311.

At June 30, 2016, the ALTCS Contract's deposits with the State Treasurer were as follows:

	Amount
State Treasurer's investment pool 3	$15,007,523
Cash	39,316,516
Total	$54,324,039

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, 2016, the State Treasurer's weighted average to maturity of its investments is 2.55 years.

Note 3 - Due from other state funds

Amounts due from other state funds at June 30, 2016, include:

- $1,173,588 of interest earned, and
- $101,865,088 of capitation and reinsurance.

Note 4 - Due from providers

The amount due from providers at June 30, 2016, is $2,162,197 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 $81,781,277 include IBNR medical claims.

Note 6 - Due to other state funds

Amounts due to other state funds at June 30, 2016, include:

- $6,095,118 of premium tax payable to the Arizona Department of Insurance and
- $36,814,703 of transfers payable to the state general fund.

Note 7 - Acute care reinsurance

During the year ended June 30, 2016, the Division received reimbursements totaling $5,160,182 from AHCCCS for acute care reinsurance expenditures for claims for enrollees incurred in 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 $7,061,560 to the health plans during the year ended June 30, 2016, and had IBNR claims of $275,000 for total acute care reinsurance expenditures of $7,336,560.

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	$ 3,438,357
Institutional care	11,821,379
Intermediate (mentally retarded)	13,384,614
Institutional care IBNR	1,724,517
Total institutional care	30,368,867
Home- and community-based services (HCBS):	
State-operated group home	6,525,383
Vendor-operated group home	260,921,795
Adult developmental home	55,920,851
Home-based services	442,456,443
HCBS IBNR	77,761,112
Total HCBS	843,585,584
Acute care:	
Acute care	148,982,479
Acute care IBNR	2,020,650
Reinsurance	7,061,560
Reinsurance IBNR	275,000
Reinsurance reimbursement	(5,160,182)
Total acute care	153,179,507
Total aid to individuals expenditures	$1,027,133,958

During the year ended June 30, 2016, the ALTCS Contract recorded allocated charges of $23,823,467 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, 2016, the ALTCS Contract recorded allocated administrative charges of $54,906,350 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 AHCCCS to pay a 2 percent premium tax on all capitation and other reimbursements paid to the ALTCS Contract. 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, 2016, consisted of $34,814,703 to the State General Fund as a result of Laws 2015, First Regular Session, Chapter 8, Section 32, and $2 million to the State-Funded Long-Term Care Fund.

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, 2016, the ALTCS Contract reimbursed the Division for $23,823,467 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 $54,906,350 of administrative and fiscal services and the Arizona Department of Insurance for $29,281,601 of premium taxes due.

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, 2016

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 6,322,274	$ 1,546,857	$ 37,904					$ 7,907,035
1st Prior		6,191,584	1,548,361	$ 29,277	$ 19,692	$ 2,029		7,790,943
2nd Prior			3,321,398	1,766,857	71,951	21,662	$ 28,132	5,210,000
3rd Prior				6,166,397	1,409,776	20,275	5,458	7,601,906
4th Prior					5,423,840	1,392,024	4,898	6,820,762
5th Prior						5,757,969	1,439,932	7,197,901
6th Prior							5,823,737	5,823,737
Total	6,322,274	7,738,441	4,907,663	7,962,531	6,925,259	7,193,959	7,302,157	48,352,284
Expenses reported	8,586,389	7,312,867	7,757,027	6,712,584	6,878,427	6,767,856	7,531,027	51,546,177
Adjustment (1)	(622,397)	471,284	(2,829,297)	1,266,969	46,832	426,103	(228,870)	(1,469,376)
Remaining liability	$ 1,641,718	$ 45,710	$ 20,067	$ 17,022	$ -	$ -	$ -	$ 1,724,517

(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, 2016

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 140,049,175	$ 71,102,025	$ 969,280	$ 337,394	$ 54,218	$ 1,042,646	$ 313,540	$ 213,868,278
1st Prior		134,421,735	70,260,457	1,063,539	346,159	189,597	(1,856)	206,279,631
2nd Prior			137,908,224	67,341,738	1,213,037	503,211	88,824	207,055,034
3rd Prior				136,663,760	39,516,490	15,829,557	3,522,758	195,532,565
4th Prior					136,590,096	68,298,348	1,082,266	205,970,710
5th Prior						123,614,517	66,302,292	189,916,809
6th Prior							128,926,617	128,926,617
Total	140,049,175	205,523,760	209,137,961	205,406,431	177,720,000	209,477,876	200,234,441	1,347,549,644
Expenses reported	216,076,777	207,215,255	213,139,553	207,153,999	192,117,881	196,301,570	196,703,639	1,428,708,674
Adjustment (1)	(9,856,579)	3,365,823	879,360	(332,440)	(14,161,190)	13,176,306	3,530,802	(3,397,918)
Remaining liability	$ 66,171,023	$ 5,057,318	$ 4,880,952	$ 1,415,128	$ 236,691	$ -	$ -	$ 77,761,112

(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, 2016

Quarter in which service was provided

Quarter of payment	Current	1st Prior	2nd Prior	3rd Prior	4th Prior	5th Prior	6th Prior	Total
Current	$ 39,770,986	$ 1,169,036	$ 463,767	$ 637,390	$ 975,443	$ 10,396	$ 4,537	$ 43,031,555
1st Prior		33,598,255	757,177	1,195,003	165,272	16,226	78,537	35,810,470
2nd Prior			38,330,782	1,146,020	283,853	79,231	22,855	39,862,741
3rd Prior				33,923,254	736,140	265,653	19,524	34,944,571
4th Prior					34,265,532	651,202	191,014	35,107,748
5th Prior						30,945,905	1,437,672	32,383,577
6th Prior							31,288,454	31,288,454
Total	39,770,986	34,767,291	39,551,726	36,901,667	36,426,240	31,968,613	33,042,593	252,429,116
Expenses reported (2)	39,133,915	42,939,633	40,776,358	35,489,783	35,162,106	37,609,908	33,404,995	264,516,698
Adjustment (1)	2,383,126	(7,909,062)	(1,106,590)	1,504,822	1,336,031	(5,637,857)	(362,402)	(9,791,932)
Remaining liability	$ 1,746,055	$ 263,280	$ 118,042	$ 92,938	$ 71,897	$ 3,438	$ -	$ 2,295,650

(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, 2016

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	$13,384,614
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	10,438,853
Department of Economic Security, Division of Developmental Disabilities and all other divisions	Administrative and fiscal services	Allocated departmental overhead costs	54,906,350
Department of Insurance	Compliance with Arizona Revised Statutes §§36-2905 and 36-2944.01	Premium tax payments	29,281,601

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

Timothy Jeffries, 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, 2016, 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 22, 2016.

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 opinion on the 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 were not 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 basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying schedule of findings and recommendations as items 2016-01 and 2016-02 to be material weaknesses.

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 2016-03, 2016-04, and 2016-05 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, and contracts, 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 22, 2016

Financial statement findings

2016-01

The Division should establish procedures to accurately record and report financial information

Criteria—The Department of Economic Security's (Department) Division of Developmental Disabilities' (Division) internal controls should include policies and procedures to help ensure that it prepares an accurate and complete *ALTCS Contract Financial Report* in accordance with generally accepted accounting principles.

Condition and context—The Department's and Division's management depend on accurate financial information to fulfill their oversight responsibility and report accurate information to the Arizona Health Care Cost Containment System (AHCCCS), the public, and other interested parties. However, the Division's *ALTCS Contract Financial Report*, composed of financial statements, related note disclosures, and other reported information contained misstatements, including mathematical errors and noncompliance with generally accepted accounting principles. The most significant misstatements were the Division understated cash and due to other state funds by $37 million.

Effect—The Division's *ALTCS Contract Financial Report* could omit important and required information or contain other misstatements. The Division made all necessary adjustments to report information in its financial statements, related note disclosures, and other reported information.

Cause—The Division used spreadsheets to account for and accumulate various financial transactions for financial reporting. The spreadsheets were prone to errors, and the review process over the spreadsheets and draft financial statements was not effective in identifying errors.

Recommendation—To help ensure that the *ALTCS Contract Financial Report* is accurate and prepared in accordance with generally accepted accounting principles, the Division should:

- Develop and follow comprehensive written procedures for compiling and presenting financial data within the financial statements and accompanying notes, including detailed instructions for obtaining information not readily available from the accounting system but necessary for financial statement preparation.
- Allocate the appropriate resources and monitor and enforce completion dates for compiling, preparing, and reviewing the financial statements and supporting schedules.
- Train other employees in financial reporting responsibilities.

- Have an appropriate employee who did not prepare the financial statements review them and the accompanying notes. The reviewer should make sure that the amounts are accurate and properly supported and the financial statements are presented in accordance with generally accepted accounting principles.

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

2016-02

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

Criteria—The Department of Economic Security (Department) should have effective internal control policies and procedures to control access to its information technology (IT) resources, which include its systems, network, infrastructure, and data. Also, the Department's policies and procedures should comply with the Arizona Department of Administration, Arizona Strategic Enterprise Technology's *Information Technology Policies, Standards, and Procedures*.

Condition and context—The Department did not have adequate policies and procedures in place to limit physical and logical access to its IT resources. Specifically, the Department's policies and procedures did not adequately address the following:

- Granting, removing, limiting, and changing employees' logical access to its IT resources. Also, the Department did not have adequate policies and procedures for periodically reviewing employee access accounts to ensure their access remained necessary and appropriate.
- Reviewing employees' network and systems access immediately when their job responsibilities change to ensure access granted is compatible with their new job responsibilities.
- Ensuring contractor and other non-DES accounts are periodically reviewed to ensure their access remained necessary and appropriate.
- Limiting the number of shared and administrator access accounts. The Department had an excessive number of shared and administrator access accounts that various employees could use to gain access. Also, auditors identified inappropriate user access accounts to the Department's network and systems that it was not aware of.
- Removing employees' network and systems access immediately upon their termination.
- Restricting physical access to its data center and periodically reviewing assigned access.
- Establishing password protection requirements for its network and systems.
- Requiring appropriate security measures for employee-owned and entity-owned electronic devices with access to the Department's network and monitoring the use of these devices. For example, the Department allows employees to connect their own devices and also provides mobile devices to some employees; however, no detailed procedures exist.
- Managing remote and wireless access, including procedures for establishing usage restrictions and configuration requirements.
- Monitoring user activity, including remote users and those users with elevated access on its IT resources.

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

Cause—Various divisions operate the Department's primary systems, and the Department lacked sufficient policies and procedures and detailed instructions for employees to follow for granting and reviewing access to its IT resources. In addition, the Department has no one dedicated to ensuring policies and procedures are written and up to date.

Recommendation—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the Department should establish effective policies and procedures that include the following:

- Granting, removing, limiting, and changing employees' logical access to its IT resources and performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with job responsibilities.
- Reviewing employees' network and systems access immediately when their job responsibilities change to ensure access granted is compatible with their new job responsibilities.
- Ensuring contractor and other non-DES accounts are periodically reviewed to ensure their access remained necessary and appropriate.
- Reviewing all shared and administrator access accounts on its network and systems to eliminate or minimize their use when possible.
- Removing employees' network and systems access immediately upon their terminations.
- Restricting data center physical access to employees who need it for their job responsibilities and periodically reviewing access granted to ensure that it continues to be needed.
- Strengthening network and system password policies by increasing the password length, requiring employees to use complex passwords and change passwords on a periodic basis, and developing a reasonable account lockout threshold for incorrect password attempts.
- Requiring appropriate security measures for employee-owned and entity-owned electronic devices with access to the Department's network and monitoring the use of these devices.
- Managing remote and wireless access, including procedures for establishing usage restrictions and configuration requirements.
- Monitoring user activity, including remote users and those users with elevated access on its IT resources.

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

2016-03

The Department should improve its information technology configuration management processes

Criteria—The Department should have adequate configuration management internal control policies and procedures to track and document changes made to its IT resources, which include its systems, network, infrastructure, and data. Also, the Department's policies and procedures should comply with the Arizona Department of Administration, Arizona Strategic Enterprise Technology's *Information Technology Policies, Standards, and Procedures*.

Condition and context—The Department has written draft policies and procedures for managing changes to its IT resources; however, they lacked critical elements. Specifically, the Department's policies and procedures did not include the following:

- Ensuring its IT resources are configured appropriately and securely. For example, the Department did not have a process to limit the functionality of its IT resources to ensure it is performing only essential services or maintaining baseline configurations for all systems.
- Establishing rollback procedures to back out changes that negatively impact IT resources.
- Preventing users with administrative access from accidently or intentionally disabling, circumventing, or altering security safeguards and other settings on their workstations. For example, the Department allows some users to have local administrator rights on their work stations, but there is no process to prevent them from downloading unauthorized software, no policy or guidance to identify what software is appropriate, and no process to monitor and detect unauthorized software.

Effect—There is an increased risk that changes to the Department's IT resources could be unauthorized or inappropriate, or could have unintended results, without proper authorization, review, testing, and approval, prior to being applied.

Cause—The Department was unaware its policies and procedures lacked critical elements and did not evaluate its policies and procedures against current IT standards and best practices.

Recommendation—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the Department should complete its written policies and procedures for managing changes and improve its configuration management processes to address the following:

- Limiting the functionality of IT resources to ensure it is performing only essential services and maintaining baseline configurations for all systems.
- Implementing rollback procedures to back out changes that negatively impact IT resources.
- Prohibiting users from making changes and bypassing the configuration management process.

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

2016-04

The Department should improve its disaster recovery plan and data backup procedures for its information technology resources

Criteria—It is critical that the Department have a comprehensive, up-to-date disaster recovery plan for its IT resources, which includes its systems, network, infrastructure, and data, to provide for the continuity of operations and to ensure that it can recover information and data in the event of a disaster, system or equipment failure, or other interruption. Also, the plan should be evaluated, tested, and updated annually. In addition, the Department's plan should comply with the Arizona Department of Administration, Arizona Strategic Enterprise Technology's *Information Technology Policies, Standards, and Procedures*.

Condition and context—The Department did not have an adequate written disaster recovery plan that included all of its systems. Also, the Department's disaster recovery processes lacked certain key elements for restoring operations, specifically:

- The plan lacked overall provisions for business continuity, including identifying essential mission and business functions and the associated requirements, maintaining essential functions despite an information system disruption, and communicating the plan to essential employees.

- The plan did not include an analysis and prioritization of recovery for key business processes, including acceptable time frames for restoring those processes.
- The plan did not include detailed procedures for moving operations to a separate site should a disaster render the data center inoperable. In addition, the Department did not have an alternate processing site for anything other than mainframe systems should a disaster render the data center inoperable.
- The Department did not keep its disaster recovery plans up to date.
- The Department did not perform regularly scheduled, comprehensive tests; document test results; and update the plan for any problems noted.
- The Department did not adequately secure and test backup data to help ensure that it is protected and can be recovered.
- The Department did not have written policies and procedures detailing the data backup procedures, including restoring the systems using the backup data in an emergency.
- The Department did not provide regular training to ensure staff would be prepared to carry out the plan.

Effect—The Department risks not being able to provide for the continuity of operations and recover vital IT resources 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 information and data and expensive recovery efforts.

Cause—The Department has some processes in place but lacks a sufficiently documented recovery plan based on current IT standards and best practices to ensure that its disaster recovery efforts and backup data can be relied on in the event that they are needed.

Recommendation—To help ensure the continuity of the Department's operations in the event of a disaster, system or equipment failure, or other interruption, the Department should:

- Conduct a business impact analysis, including recovery objectives, restoration priorities, and metrics, to evaluate the impact that disasters could have on its critical business processes and revise its disaster recovery plan to include the analysis' results.
- Develop and document procedures for migrating critical information system operations to a separate alternative site for essential business functions. Put contracts in place or equip alternate site to resume essential business functions, if necessary. Information security safeguards at the alternative site should be equivalent to the primary site.
- Ensure that its disaster recovery plan is updated for all critical information.
- Develop and document a process to perform regularly scheduled tests of the disaster recovery plan and document the tests performed and results. This process should include updating and testing the disaster recovery plan at least annually or as changes necessitate. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. Test results should also be used to update or change the plan.
- Establish and document policies and procedures for testing backups of IT systems and data to help ensure that the Department could recover them in the event that they are needed. Policies and procedures should require data backups to be protected.
- Improve its existing written policies and procedures to ensure they are sufficiently detailed to address backing up and restoring data.
- Ensure the plan addresses how to communicate changes to key personnel.
- Develop and implement an ongoing training schedule for staff responsible for implementing the plan. In addition, ensure the training provided is specific to the user's assigned roles and responsibilities.

This is similar to prior-year finding 2015-01.

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

2016-05

The Department should improve security over its information resources

Criteria—To effectively maintain and secure financial and sensitive information, the Department should establish internal control policies and procedures that include practices to help prevent, detect, and respond to instances of unauthorized access or use, manipulation, damage, or loss to its IT resources that are based on acceptable IT industry practices. Also, the Department's policies and procedures should comply with the Arizona Department of Administration, Arizona Strategic Enterprise Technology's *Information Technology Policies, Standards, and Procedures*.

Condition and context—The Department did not have written policies to help secure its IT resources and did not adequately secure its IT resources. Specifically, the Department did not:

- Develop a department-wide IT security risk assessment process that is performed on a periodic basis or at least annually and includes documentation of results, evaluation by appropriate individuals, and prioritization of risks identified for remediation. In addition, any threats identified as part of the Department's IT security vulnerability scans should be incorporated into this IT security risk assessment process.
- Identify and classify data by sensitivity and take appropriate action to protect sensitive information.
- Establish a process to perform external and internal monitoring of its information systems.
- Establish a process to respond to security incidents.
- Use updated software for all its systems. Specifically, the Department was using outdated and unsupported software that may have been vulnerable because the vendor no longer provided security updates to protect against malicious attacks.
- Provide a fully developed security awareness program for its employees, nor did it have a training program to help ensure they were familiar with the Department's IT security policies and procedures.
- Have a process to identify vulnerabilities in its IT resources on a periodic basis, nor did they have a plan to prioritize and remediate or mitigate identified vulnerabilities.
- Properly manage its IT vendors, such as providing guidance for procurement of IT vendor services that require consideration of IT risks, costs, benefits, and technical specifications; monitoring of vendors to ensure conformance with Department contracts; and ensuring sensitive data is properly secured and protected.
- Have an adequate process or documented policies and procedures to ensure patches are applied to all IT resources.
- Have a policy or process for protecting digital and nondigital media.

Effect—There is an increased risk that the Department may not prevent or detect unauthorized access or use, manipulation, damage, or loss to its IT resources.

Cause—The Department was unaware its policies and procedures lacked critical elements related to IT security and did not evaluate its policies and procedures against current IT standards and best practices.

Recommendation—To help ensure that the Department is able to effectively maintain and secure its IT resources, the Department should develop written policies and procedures over securing its IT resources. Those policies and procedures should include the following:

- Conducting an IT security risk assessment process periodically or at least annually that includes documentation of results, evaluation by appropriate individuals, and prioritization of risks identified for remediation. Also, any threats identified as part of the Department's IT security vulnerability scans should be incorporated into this IT security risk assessment process.
- Identifying, classifying, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to that information.
- Performing external and internal monitoring of its information systems.
- Responding to security incidents. This process should include developing and testing an incident response plan and training staff responsible for the plan. These policies and procedures should include following regulatory requirements and making disclosures to affected individuals should an incident occur.
- Establishing a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- Providing a comprehensive training program for all employees on security awareness and the Department's security policies and procedures.
- Conducting vulnerability assessments that include performing IT security scans on a periodic basis and responding to identified threats by prioritizing and remediating or mitigating identified vulnerabilities.
- Monitoring IT vendor's performance to ensure conformance with department contracts and securing and protecting sensitive information and data from the IT vendors.
- Ensuring patches are applied to all IT resources.
- Protecting digital and nondigital media.

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

This page is intentionally left blank.

DIVISION RESPONSE

Douglas A. Ducey
Governor

DEPARTMENT OF ECONOMIC SECURITY
Your Partner For A Stronger Arizona

Timothy Jeffries
Director

November 21, 2016

Debra Davenport
Auditor General
2910 N. 44th Street, 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 the Government Auditing Standards. Specifically, we are providing you with the names of the contact people responsible for the corrective action, what activities are planned and the anticipated completion date.

Please let me know if you have any questions regarding these corrective actions.

Sincerely,

Joseph Tansill
Business Operations Administrator

Attachment: ALTCS Financial Statement Audit Corrective Action Plan (5 pages)

cc: Dr. Laura Love, DDD Assistant Director
Lisa Cavazos-Barrett, DDD Deputy Assistant Director
Ben Kauffman, DDD Finance Manager
Sherri Wince, DDD Corporate Compliance Officer

2016-01
The Division should establish procedures to accurately record and report financial information

Name of contact person and title: Joseph Tansill, Division of Developmental Disabilities Business Operations Administrator

Anticipated completion date: January 31, 2017

The Department agrees with the finding and provides the following corrective action plan.

1. Develop and follow comprehensive written procedures for compiling and presenting financial data within the financial statements and accompanying notes, including detailed instructions for obtaining information not readily available from the accounting system but necessary for financial statement preparation.
    - Due to the implementation of the new statewide financial system, the Division has begun to review the procedures and processes associated with the preparation of the financial statement. This review will include the following items:
        - Review and update spreadsheets used to account for and accumulate financial transactions
        - Update desk procedures related to preparation and presentation of financial statements
        - Document criteria, policy, and guidelines to ensure that proper reporting occurs each quarter in accordance with generally accepted accounting principles
    - The Division will continue to review and update the documented procedures to ensure compliance.

2. Allocate the appropriate resources and monitor and enforce completion dates for compiling, preparing, and reviewing the financial statements and supporting schedules.
    - The Division will develop a standard timeline for compiling, preparing, and reviewing the financial statements and supporting schedules to allow appropriate review time for individuals with the Department.

3. Train other employees in financial reporting responsibilities.
    - Once process and procedures are documented and implemented, the Division will cross-train staff to ensure multiple staff have the ability to complete the financial statements.

4. Have an appropriate employee who did not participate in the financial statements review them and the accompanying notes. The reviewer should make sure that the amounts are accurate and properly supported and the financial statements are presented in accordance with generally accepted accounting principles.
    - The Division will implement a review process after the completion of the financial statements to include individuals that possess the required technical knowledge who were not part of the preparation of the documents to review for accuracy. This

process will be used to reduce mathematical errors and noncompliance with generally accepted accounting principles.

2016-02
The Department of Economic Security should improve access controls over its information technology resources
Name of contact person and title: Jeffrey Raynor, DES Chief Information Security Officer
Anticipated completion date: June 2017

The Department agrees with the finding and provides the following corrective action plan.

The department has just completed its review of policy 1-38-8320, Access Control on October 21, 2016. It anticipates that that policy will be published in November 2016. Work has already begun on the associated procedure (1-38-8320.01) which will address concerns raised in this audit. It is anticipated that this procedure will be published and in effect by the end of January 2017. Specifically, the procedure covers (among other topics):

- Granting, removing, limiting and changing employee, contractor, and partner logical access to information systems.
- Limiting privileged accounts
- Periodically and immediately upon transfer, termination, or change in job duty; review employee, contractor, and partner logical access to information systems.
- Wireless or remote access to information systems.

Upon completion of the project to move the data center in September 2016, the department implemented extremely restricted criteria for physical access to the data center. The department will commit those changes to a detailed procedure that will become a part of Procedure 1-38-8260.01 Physical Security of Information Systems Procedure that is scheduled to be published in the first calendar quarter of 2017. In the interim, the department will publish a temporary procedure specific to the physical security controls for the IO Data Center.

The department finalized policy 1-38-8325, Mobile Device Management on August 2, 2016, along with a set of standards for mobile devices, remote access, and data storage on mobile devices. This set of policy establishes the department's security controls relating to mobile devices whether owned by the state or the employee. However, it should be noted that management has decided not to purchase an enterprise mobility management product, and therefore will be revising this policy and procedures to reflect these new standards and references. The policy and procedures are expected to be completed by the end of February 2017.

DES Policy 1-38-8330, System Security Audit Policy is currently being reviewed. It is expected that the policy will be comprehensively revised and published before the end of 2016. It along with the System Security Audit Procedure will define the manner in which the department audits logs of remote users and users with privileged access.

2016-03
The Department should improve its information technology configuration management processes
Name of contact person and title: Jeffrey Raynor, DES Chief Information Security Officer
Anticipated completion date: January 2017

The Department agrees with the finding and provides the following corrective action plan.

The department has drafted a comprehensive policy and procedure for change management. As a result of the department's policy reduction program, those policies were identified to be included in the System Security Maintenance Policy. The configuration change policy has already been integrated into DES Policy 1-38-8220, System Security Maintenance which was finalized on September 23, 2016. The change management procedure is also complete and will be integrated into the System Security Maintenance Procedure (1-38-8220.01) by the end of January 2017.

2016-04
The Department should improve its disaster recovery plan and data backup procedures for its information technology resources
Name of contact person and title: Jeffrey Raynor, DES Chief Information Security Officer
Anticipated completion date: February 2017

The Department agrees with the finding and provides the following corrective action plan.

DES is in the process of reviewing its disaster recovery process. The department finalized its contingency planning policy on October 21, 2016, which calls for disaster recovery plan along with associated testing, training, and documentation.

DES has allocated a position for a disaster recovery coordinator and is currently recruiting for a candidate. This position will assist with the maturation of this program. In conjunction with the department's risk assessment program, a comprehensive effort is underway and nearly complete to identify and document each of the department's distributed, mainframe, and cloud information systems. The effort is currently in the phase of identifying each network resource associated with these system and documenting these system with tables showing resources, system ownership, and documentation of the sensitivity of data contained on each system. Data flow diagrams will be constructed for each system.

In December 2016, the effort will begin, again – in conjunction with the risk assessment program, to assign a criticality level to each system.

Beginning in January 2017, beginning with the systems identified as most critical, documentation of the systems' disaster recovery plans will begin. Some existing plans are mature such as those on the mainframe. Others are poorly documented. Once documented, each systems DR plan will be evaluated and determinations will be made based upon the completeness of the plan and the thoroughness of the DR plan to determine what DR gaps exist. It is recognized that filling these gaps may require significant expenditures and those will be examined and prioritized. As viable plans emerge, testing will begin. As the testing identifies further gaps, those will be addressed based upon system criticality and budget. When approved

plans emerge, training will begin. The department expects the most critical systems to have final tested plans by the end of 2017.

The department has issued a purchase order for an enterprise backup solution. This solution will be implemented by the end of January 2017, and will finish the department's effort to have viable and complete backups of all CIF shares and data within the environment.

2016-05
The Department should improve security over its information resources
Name of contact person and title: Jeffrey Raynor, DES Chief Information Security Officer
Anticipated completion date: February 2017

The Department agrees with the finding and provides the following corrective action plan.

The department has recently published its Risk Management policy which calls for annual assessments of each of the department's 200 IT systems along with common infrastructure systems. Those systems that process confidential information are scheduled for annual reviews as it the common infrastructure. The remaining parts of the risk management structure are currently being finalized and consist of the Risk Management Procedure, Risk Management Schedule, and the risk management reporting.

As a precursor to the risk assessment process described above, data on each system will be identified and classified. The risk assessment procedure calls for each system to identify what type of information (from the Data Classification Policy, 38-8110) the system processes. Infrastructure-wide systems are considered to process all classifications of data. The process to associate data classifications with systems is underway and nearly complete. This will be a major factor in determining which systems will be addressed in the first wave of risk assessments which will begin in January 2017.

DES has established in policy 38-8130, the framework in which the agency's Security Plan will exist. The Security Plan is in the process of being written and will be published before the end of calendar year 2016. Although DES has many systems in place for performing internal and external monitoring of applications and infrastructure, those are not yet documented. The Security Plan will accomplish that task.

DES has an Incident Response Policy, 38-8240. It is currently finalizing the Incident Response Procedure/Plan which will be in place by February 1, 2017. That procedure will outline the manner in which DES responds to all information technology related incidents.

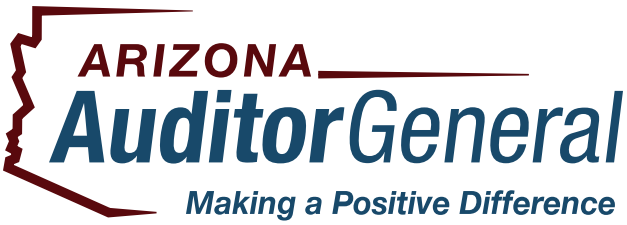
DES has a policy, 38-8220, System Security Maintenance which mandates that all software used in the agency be approved by the CIO and that it is supported by the manufacturer. DES has identified all non-compliant software and is working to remediate software that is non-compliant. The program is targeting software installed on devices that process sensitive data ahead of other software and has made great progress in remediation. Just this week, two Microsoft Windows 2003 Servers are being decommissioned having already been replaced by Microsoft Windows 2012 Servers. The formal risk assessment program described above will document unsupported software in use and will associate it with specific systems and data sensitivity levels. A formal system authorization will be required for each system that will require

upgraded software or compensating controls sufficient to overcome the risk of unsupported software.

The agency conducts security awareness training annually for all employees. Beginning in 2017, that training will be expanded to require formal role-based security training. The security policies and procedures were previously published and available on the department's intranet. Beginning in August 2016, Information Risk Management began a program to modernize its security policy. A dedicated policy and procedure position was created and filled with a policy and procedure specialist. A SharePoint site was created and dedicated to IT policy. Policies were consolidated to reduce over 100 documents to 18 polices and approximately 20 procedures. Those policies will be indexed to make it easier for users to find specific policy guidance. This new policy system will be presented as a part of role based security training beginning in 2017.

Although DES has a vibrant program to scan the network for vulnerabilities both by use of internal scanners and contracted penetration testing, the procedure to document that process is not yet mature. DES also has an active process to remediate vulnerabilities by patching, decommissioning non-compliant software or hardware, installing required software, or putting system-wide controls in place to neutralize the vulnerability. The Information Security Plan 38-8120.01 is currently being written and will describe this information in detail. It is scheduled to be published in December 2016.

DES has recently revised its vendor management process and software acquisition process to include a risk assessment performed by Information Risk Management, Enterprise Architecture, Server Operations, and Service Delivery before each purchase. Previously that process was only performed on systems with a cost of over $25,000.


ARIZONA
Auditor General
Making a Positive Difference