

# Large-Scale Computing Systems Study

Presented to: Governor Janice K. Brewer, Secretary of State Ken Bennett,  
President of the Senate Andy Biggs, Speaker of the House Andy Tobin  
and the Senate and House Appropriation Committees



Prepared By: Arizona Department of Administration (ADOA)  
Arizona Strategic Enterprise Technology (ASET)  
Date Submitted: October 1, 2014\*

*\*Document citation links may not be valid after this date*

# Table of Contents



Executive Summary .....	3	Cloud Computing.....	65
Scope Definition – Large-Scale Computing System (LSCS) Study.....	9	Overview .....	65
LSCS Study Methodology.....	13	Strategy – Promote Cloud as Viable Alternative to Ownership.....	66
IT Inventory .....	13	Detailed Analysis .....	67
Data Center Survey.....	13	Arizona Network (AZNet II).....	71
Research .....	14	Overview .....	71
Data Collection .....	14	Strategy – Provide Core Telecom and Network Infrastructure; Refresh the	
Case Study .....	14	Entire Network .....	71
Large-Scale Computer System (LSCS) Study .....	17	Detailed Analysis .....	72
IT Security.....	18	Enterprise Capabilities.....	75
Overview .....	18	Overview .....	75
Strategy – Systematically Address Security Issues .....	19	Strategy – Expand Adoption of Secure Statewide Enterprise	
Detailed Analysis .....	20	Capabilities.....	76
Mainframe Utilization.....	29	Detailed Analysis .....	77
Overview .....	29	IT Personnel.....	89
Strategy – Manage Capacity, Costs and Resources .....	30	Overview .....	90
Detailed Analysis .....	31	Strategy – Develop Dynamic Programs to Recruit and Retain	
Server Utilization .....	45	IT Talent.....	90
Overview .....	45	Detailed Analysis .....	91
Strategy – Move from Physical to Virtual or Cloud		IT Governance and Funding.....	101
and Reduce Cost and Risk .....	47	Robust IT Governance .....	102
Detailed Analysis .....	48	Automation Project Fund (APF) .....	102
IT Facilities .....	52	Federally Disallowed Expenditures .....	110
Overview .....	52		
Strategy – Assess Existing IT Facilities; Justify Continuity			
or Remediation .....	53		
Detailed Analysis .....	54		

# Executive Summary



In 2012, the Arizona Legislature passed a law requiring the Arizona Department of Administration (ADOA) to complete a statewide study of large-scale computing systems. The law defined specific elements to be included in this study, including Arizona's current use of, reliance on, and costs of, its current large-scale computing systems. In addition, ADOA was required to highlight specific, comparable systems available in the market and the feasibility of leveraging those systems, or services, to potentially lower overall costs, increase necessary computing capacity, and reduce risk. The Arizona Department of Administration (ADOA) – Arizona Strategic Enterprise Technology (ASET) division completed the research and analysis necessary to compile the report and has included its findings and recommendations for consideration to the appropriate decision-makers.

In order to meet the requirements of this report, ADOA-ASET utilized a variety of sources of information. One source used was the Information Technology (IT) inventory tracking system which is currently maintained by ADOA-ASET. IT inventory is a database that includes a list of all Information Technology assets owned, leased or employed by the State in accordance with ARS § 41-3405.A.1.(e). The process for collecting this data annually requires eighty-nine Executive Branch agencies to submit a list of their assets to ADOA-ASET.

ADOA-ASET also conducted a survey with eighty-nine Executive Branch agencies to gather information regarding the data centers and server rooms currently maintained by the agencies. These facilities house the technology equipment necessary to manage and support large-scale systems and applications. Sixtyone agencies responded to the survey and a summary of the findings are included in this report. ADOA-ASET staff assisted agency IT personnel with asset data submission, and reviewed agencies' Project Investment Justifications (PIJs) as part of fulfilling the requirements of this law.

This report covers a variety of areas including the current utilization of the State's mainframe and server-based systems, the State's strategy for cloud computing, and the status of the State's network and security capabilities. In addition, detailed information has been provided regarding the State's Digital Government program and the positive impact recent investments in this area have had on the State. And finally, it includes a summary of the challenges the State is currently facing regarding the recruitment and retention of its IT personnel.

Arizona State Government is a large, complex entity and its IT footprint across the State is extensive. For example, over 32,000 employees across more than 670 buildings use IT services. The state currently employs over 1,450 full-time IT employees and more than 400 IT contractors to provide those services. The statewide telephony and data network that helps provide these IT services handles more than 500,000 telephone calls and three terabytes (3TB) of data on a daily basis. Billions of dollars in transactions are processed yearly on the mission-critical systems maintained by state agencies and over \$850 million in IT projects are being executed currently to ensure the State IT systems are operational and secure.

Given the size and complexity of State Governments, it is no wonder numerous states have suffered cyber security breaches the past several years. ADOA-ASET has been systematically identifying, prioritizing, and remediating security issues in various agencies over the past three years. One key observation is that this approach will not work. It does not scale fast enough, and it will take far too long to reach the more than 132 state agencies and resolve their disparate issues. To protect the State, more aggressive steps must be taken.

As a result of this report, ADOA-ASET has determined that information technology is a critical component of how the State operates. Although other states such as Utah, North Carolina, Michigan, and Massachusetts have leveraged such assessments to drive IT consolidation, Arizona has a unique set of challenges and state leadership must consider a wide variety of options to determine which will, ultimately, have a positive impact on the State.

Protecting citizen data is one of the highest priorities of the State. However, cyber threats continue to increase drastically each year, in number and complexity. The state currently tracks and blocks more than 8,000 malicious attacks against state systems on a daily basis. The email system at the Arizona Department of Administration alone receives more than 100,000 malicious emails daily. Today, there are widely different levels of security controls implemented for agencies and data centers. In addition, there is a lack of resources and knowledge to identify security risks, especially in smaller agencies, boards and commissions. In order to mitigate the security and privacy risks the State is facing today, a more centralized approach is necessary.

The State currently operates three mainframe computing systems that host many of the largest and most critical applications. The Department of Public Safety and Department of Economic Security mainframes are dedicated to their respective agencies. The Department of Administration (ADOA) operates a mainframe for hosting applications used statewide and hosts applications for eight entities. There are 228 applications operating on the three state mainframes of which 77 are assessed by their agencies as Low or Medium functional adequacy.

Mainframes are extremely expensive to procure and maintain. The ADOA-ASET mainframe alone will incur estimated software costs of \$8,525,000 in fiscal year (FY) 16. The modernization of these statewide mainframe applications should eventually be considered, however there will be significant costs associated with the rewriting of those applications. Finally, mainframe resources, particularly programmers, are limited and are expected to be harder to find in the future. The State must have a long-term strategy for recruiting and retaining these valuable resources, including the possibility of pooling statewide resources.

In addition to mainframes, the State also supports and maintains distributed server infrastructures. It has been determined that 61 of the state budget units in the Executive Branch operate at least 2,576 servers in a variety of IT facilities. Currently, the total reported initial cost of all servers, in the State, is approximately \$26,450,000.

Although many agencies are taking advantage of server virtualization capabilities, it still requires significant upfront capital expenses to deploy. In addition, while moving to virtual servers can reduce the overall number of system administrators required to manage the total number of physical servers, it also requires increased skills to take advantage of the more robust solution. On the other hand, while cloud may be one of the biggest IT buzzwords, leveraging cloud capabilities is quickly becoming a better option than on-premise, physical or virtual servers.

There are a significant number of advertised advantages associated with cloud computing including potential reduction of IT capital expenditures and recurring costs. These apparent advantages are consistent with the analysis completed as part of this report. As an example, a shared, on-premise, email service with 50GB storage per user per month currently costs \$152, while a hosted email exchange solution Microsoft offers costs only \$4. In general, there are many benefits to moving specific services to the cloud and the State should continue to identify, assess, and potentially pursue those opportunities in the future.

ADOA-ASET provides a shared services infrastructure that is secured, optimally virtualized, and scalable for many state agencies today. ADOA-ASET is constantly working with agencies to evaluate which systems can be virtualized, moved to cloud services, or need to remain on-premise. This report has been one of the main catalysts for ADOA-ASET to move its services to the cloud. As it assessed its physical and virtual infrastructure, ADOA-ASET considered total cost of ownership, evaluated capital expenses vs operational expenses, cost models, and looked to address the difficulties associated in securing capital funding for new equipment. As a result, ADOA-ASET has successfully migrated many of its services to the cloud including email, website hosting, and specific security services, and will continue to migrate more services over time.

Technology is critical for continuity of government services and can also be a transformer to enable State Government to better serve its stakeholders. While it is critical to develop sustainable IT strategies that ensure the continuity of government, it is equally important for the State to adopt modern technologies

to keep pace with ever-increasing demands of its citizens and businesses. A balance between running the business and changing the business must be maintained from both budget and human capital perspectives.

The State's Digital Government program is the key to future innovation that can truly change the way the State provides services. ADOA-ASET currently manages the state's Digital Government program and supports 95 State agencies and over 150 websites or applications. The Digital Government platform provides a secure payment engine (i.e. credit card payment system) to public entities. This payment engine processes approximately 427,000 transactions and over \$70 million in revenue per year. The program is in the process of implementing a statewide single sign-on system that will be first used when the new accounting system comes online in July 2015. This single sign-on system will be a high-value enterprise component that state agencies can leverage as they integrate their systems to increase the secure user identity and access management processes.

From an IT personnel perspective, the State is currently facing a looming crisis due to the fact that over 27 percent of its full-time IT employees are eligible for retirement over the next five years. In addition, the State is constantly challenged with overall IT salaries historically being lower than in the private sector. Finally, due to budget constraints, centralized training offerings have been either minimized or eliminated altogether. Despite the challenges, the State has taken on several initiatives to improve recruiting and retention of IT employees over the past few years. The State should continue to invest in high quality, effective, IT training, Centers of Excellence, and Apprenticeship programs to keep up with skill requirements.

The federal government often enlists state governments as partners through federal financial participation in a variety of programs. The federal government maintains equity shares in the funding streams and closely monitors the expenditure of enterprise fund activities. In many cases, the federal government determines that specific state expenditures are disallowed, and monies collected for disallowed purposes must be returned to the federal government.

This issue absolutely impacts planning and acquisition of large-scale computer systems. ADOA-ASET has been working with the General Accounting Office (GAO) on this issue for several years. One strategy being deployed to avoid disallowed costs is to lease large-scale systems. ADOA-ASET is also working with the State Procurement Office (SPO) to ensure that the State has the right contracts to enable these types of purchases and to avoid the disallowed cost issues.

In conclusion, ADOA-ASET has benefited from lessons learned through efforts of others states to increase IT efficiencies, capabilities, and reduce costs. It has also chartered a course to address the key IT challenges facing the State. The strategy includes robust and scalable security, capacity utilization, shared service along with increased service reliability, reduced risk and a visionary personnel development program.



# Scope Definition

## Large-Scale Computing System (LSCS) Study



Laws 2012, Fiftieth Legislature, Second Regular Session Chapter 161, Section 1, required Arizona Department of Administration (ADOA) to complete a Large-Scale Computing Systems (LSCS) study.

The Law defines the following elements to be included in the study:

- This state's current use of, reliance on, and costs of large-scale computing systems and the potential cost savings from, and potential consequences of, employing other large scale computing systems that are available in the marketplace. The study shall consider:
  - The nature of the operations supported by existing large-scale computing systems, including this state's need to conduct those operations in a reliable, secure, scalable and end-user-friendly manner
  - For existing large-scale computing systems, employee costs, one time charges, recurring charges and average maintenance charges associated with the components of large-scale computing systems
  - For existing large-scale computing systems; this state's reliance on employees from the private sector for system maintenance and support and the feasibility of having those functions performed by new or existing state employees
  - An assessment of the overall value of existing large-scale computing systems to this state
  - Whether large-scale computing systems of comparable capacity and performance characteristics are available in the marketplace and, if not, in what manner the marketplace is failing to offer these comparable systems

- If comparable large-scale computing systems exist in the marketplace; what good faith estimates exist for cost components comparable to those existing large-scale computing systems
- If comparable large-scale computing systems exist in the marketplace; the feasibility of having system maintenance and support functions performed by employees of this state
- Whether large-scale computing systems exist that might provide this state with overall value comparable to, less than, or greater than, existing large-scale computing systems.
- The number of public documents that are available on the internet and the potential cost savings that could be obtained by making more documents available on the internet. Any recommendations that result from this study shall require that state documents and information use nonproprietary industry sitemap protocols and search engine mapping.

The law defined “Large-Scale Computing Systems” as:

- A computer, or a designated network of computers, that in daily operation:
  - Supports, or is capable of supporting, more than ten million transactions per hour, or is used to store more than one hundred billion bytes of data generated by this state; or
  - Is used for critical computing needs, including bulk data processing, transaction processing, resource planning, statistic generation, process monitoring and process modeling.
- The applications, operating system and other support software, hardware add-ons and maintenance services required by the operating system.

The law also defined “Overall value” to include factors such as total cost of ownership, the quality of

hardware, software or services to be delivered by contractors supporting a large-scale computing system, the contractor’s responsiveness and account service record, and a contractor’s willingness to share risk.

Similar legislation and outcomes from other states were considered to gain background knowledge about their approach. While similar legislation was introduced in at least four other states (Louisiana, Maryland, Illinois and New Jersey) in recent years, the outcomes varied.

Arizona’s LSCS study differs from the other states, in that it characterizes a Large-Scale Computing System as capable of storing 100GB (100 billion bytes) of data, whereas in other states, the storage stipulation was one terabyte of data (1 trillion bytes). This makes the Arizona legislation far more inclusive, to the point that virtually any computer used by State agencies would be considered a large-scale computing system if it were used for critical computing.

This difference is so significant that it bears highlighting the conclusions of the Maryland Department of Legislative Services (Fiscal and Policy Note) related to the storage stipulation in their less inclusive 2008 legislation:

**Background:** *Each of the 63 executive agencies in the State uses thousands of computers, most of which are networked. Certain agencies, such as the Maryland Department of Transportation, employ vast amounts of computing power on a daily basis. In addition, one terabyte of computer data storage (for example, two 500 gigabyte hard drives) can currently be purchased for less than \$500.*

**State Expenditures:** *The study required by the bill encompasses an enormous range of computer systems from every Executive Branch agency. In order to analyze these systems in the manner and short timeframe required by the bill, the Department of Budget and Management Office of Information Technology advises that it would have to hire an outside contractor at an estimated price of \$1,808,000<sup>1</sup>.*

<sup>1</sup>Department of Legislative Services, Maryland General Assembly. (2008). “House Bill 1226”. [Fiscal and Policy Note]. Retrieved from [http://mgaleg.maryland.gov/2008rs/fnotes/bil\\_0006/hb1226.pdf](http://mgaleg.maryland.gov/2008rs/fnotes/bil_0006/hb1226.pdf)

<sup>2</sup>“State agencies” and “agencies” are used synonymously with Budget Unit: Arizona Revised Statutes 41-3501 provides the following definition of a Budget Unit:

*“Budget unit” means a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona board of regents but excluding the universities under the jurisdiction of the Arizona board of regents, the community college districts and the legislative or judicial branches.*

Rather than focusing on the storage capacity of computer systems, an assumption was made to not include an individual’s laptop or desktop computer in the LSCS study scope but to instead focus on the State’s true large-scale systems.

It is noteworthy that multiple states including Utah, North Carolina, Michigan and Massachusetts have leveraged such assessments to drive Information Technology consolidation. Upon further review, the major value from such initiatives was gained on projects including, statewide enterprise systems for accounting, human resources, and procurement, as well as implementing statewide telecommunications and network systems and consolidating the number of mainframes. These projects have yielded high returns for many states, including Arizona, which has already implemented each of these strategies.

The LSCS study has included eighty-nine (89) state agencies<sup>2</sup> in the Executive branch for which the Department of Administration has statutory authority for strategic IT asset oversight.

# LSCS Study Methodology



The Arizona Department of Administration (ADOA) – Arizona Strategic Enterprise Technology (ASET) division utilized processes and resources already available under statutory authority in order to respond to the reporting requirement of this bill and leveraged the following four tools and methods for the LSCS study:

## **IT Inventory**

ADOA-ASET currently maintains a list of all Information Technology assets owned, leased or employed by the State in accordance with ARS § 41-3405.A.1.(e). The process for collecting this data requires 89 Executive Branch agencies to submit a list of their assets to ADOA. The list of assets is loaded into a database and used for reporting. The data collection is a 6-month process which involves agencies performing automated or manual collection, reconciliation, correction, approval and submission of data. This is followed by extensive review of the data, profiling for data accuracy and quality and preparing the data for reporting.

In preparing for the 2014 data collection cycle, data collection parameter were modified to consider the additional requirements dictated by the LSCS study. Agencies were given an additional three months for their submissions.

The IT Inventory data collection process also gathers information about state computer applications, including criticality, functional adequacy, and life cycle stages.

## **Data Center Survey**

Large-scale computing systems are housed in data centers or server rooms. Due to the federated IT environment in the State of Arizona, state agencies have historically maintained IT equipment within areas typically controlled by them. ADOA-ASET conducted a survey of all 89 agencies to gather the

number, size and usage statistics of IT facilities in the State. The survey queried state agencies in areas ranging from floor space to number of data centers, their tiers, utilization, and planned upgrades. The results from this survey augmented and complemented the information that is not currently collected through IT Inventory. In order to better control and measure the results, a range of potential responses were allowed. The responses were designed to give us a consistent view of the infrastructure.

### **Research**

ADOA-ASET researched similar legislation and trends in Federal and State Governments and reviewed relevant case studies that were publicly available. ADOA-ASET studied usage of this state's mainframe and other major applications, ongoing projects and Project Investment Justification (PIJ) documents.

### **Data Collection**

Discussions were conducted with Chief Information Officers (CIOs) of major state agencies and key personnel to solicit their feedback, plans and strategies. A standard questionnaire was used to guide the discussions. Follow up visits to some of the agencies was done to provide further clarification around identifying appropriate equipment and software for reporting purposes. Equipment categorization was done jointly with some of the agencies to achieve consistency in reporting. ADOA-ASET also held webinars to explain the data collection process which included several iterations of data submissions to eliminate data errors.

### **Case Studies**

In 2011 Oklahoma delivered the "Information Technology and Telecommunications Transfer, Coordination, and Modernization Study" based on House Bill 1170. Oklahoma worked with Capgemini Government Solutions LLS<sup>3</sup>, to develop this assessment. Throughout the LSCS study, references to multiple states have been included. ADOA-ASET made direct comparisons to the Oklahoma study as baseline for this report. Upon review ADOA-ASET determined that the conditions in that state, were comparable to Arizona at the time the report was delivered. Oklahoma's IT was a federated function at the agency level with 109 agencies serving a population of 3.7 million residents compared to Arizona's 132 state

---

<sup>3</sup>Capgemini Government Solutions LLC., developed by, <http://www.ok.gov/cio/documents/ITModernizationStudy01042011.pdf>

agencies serving 6.6 million residents. Based on these numbers, the FY 13 budgets, and structural deficits at \$6.8 billion and \$600 million respectively, were comparable to Arizona's \$8.8 billion and \$1 billion. The strategy prescribed in Oklahoma's assessment called for a long-term solution to offset the state budget reductions at that time, while providing ongoing savings and cost containment. Sustainability, standardization, simplification and scalability were the other key points raised in the study that offered a comprehensive roadmap in areas targeted for improvements. Oklahoma's report also noted that duplicative expenditures in core IT infrastructure will only result in larger future cuts.

Arizona has adopted a similar multi-pronged approach over the past three years. Arizona's approach to IT security, mainframe and server utilization, IT facilities, use of the maturing cloud options, Arizona Telecommunications Network, Enterprise Capabilities, IT Personnel and IT Funding show strong parallels to the recommendations contained in the report. The inefficiencies highlighted in the decentralized IT model are common to both the states. The federated approach results in the inability to leverage buying power across the enterprise. The agencies risk capacity and facility over-provisioning as a result of the need to accommodate temporary surges. Agencies are however taking advantage of technology to automate processes to drive down manual costs. In an innovation driven society, IT is the vehicle to invest in to augment agency missions. In the area of data sharing among agencies, a great start has been made in the area of security, cloud and enterprise capabilities which now must have the support of policy makers and agency leaders for further adoption in a systematic manner. The issues related to non-uniformity in continuity of operations and disaster recovery are similar to Oklahoma. The current economic recovery poses a challenge by putting the State in direct competition with the private industry with regards to recruiting talented IT professionals. Arizona has adopted an assertive strategy of finding, retaining and training key IT personnel in a bid to address both agency and citizen needs in a highly technology driven environment.

There are differences in the strategies adopted between the two states, the key differentiators being Arizona putting a priority on operational excellence, innovation and transformation, IT governance, and proactively managing IT risk. To ensure better alignment between strategy and execution, Government

Information Technology Agency (GITA), an IT strategy focused agency, was merged into ADOA, an agency responsible for providing IT services across the state agencies. Further opportunities abound in the realm of infrastructure and application standardization including storage, imaging, cloud solutions and application rationalization which can reduce or avoid costs, and allow investments to be channeled to further reduce IT security risks and improving efficiencies in service delivery. Moving forward, Arizona should continue to mature areas such as IT Service Management, Project and Program Management, Configuration Management, Asset Management, and system and application monitoring.



# Large-Scale Computing Systems (LSCS) Study





## Overview

- A. 100,000+ malicious emails received daily by the ADOA system, which equates to 96 percent of overall traffic.
- B. 1,000,000+ malicious attacks daily to all state employees while browsing the internet.
- C. 8,000+ malicious attacks daily against state systems.
- D. 20+ SQL injection attacks daily against state web servers.
- E. 10+ Multi-state Information Sharing and Analysis Center (MS-ISAC) alerts daily.
- F. 800+ Trojan attacks.
- G. Different levels and diverse security controls, or lack thereof, in different agencies and data centers.
- H. Lack of resources and knowledge to identify security risks, options and impact within many small agencies, boards and commissions.
- I. Security policies, framework and standards based on National Institute of Standards and Technology (NIST) and National Cyber Security Framework, Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS) Publication 1075, and Payment Card Industry (PCI).
- J. ADOA offers 84 different security controls for network, data center, and cloud services. Twelve of these controls are operational statewide services.

- K. Cyber-threats continue to increase each year in number and complexity. Multiple state and local governments have been victims of cyber-breaches including Utah in 2012 (750,000 records; cost of \$9,000,000), South Carolina in 2012 (3.8 million records; cost of \$40,000,000+), Oregon in 2014 (337,000 records; cost of \$177,000), Maricopa Community College in 2013 (2.3 million records; cost of \$20,000,000+), Montana in 2014 (1.3 million records; cost up to \$2,000,000), North Dakota University in 2014 (290,000 records; undetermined cost), University of Maryland in 2014 (300,000 records; undetermined cost), Indiana University in 2014 (146,000 records; undetermined cost).
- L. Need for cyber analysts to monitor and analyze cyber-attacks in order to lower the risk of data exfiltration.
- M. Creation of a security program to monitor cyber security attacks, activities, vulnerabilities, and to measure and close security gaps.

**Strategy – Systematically Address Security Issues**

Government is a prime target for malicious attacks due in-part to the large quantity of sensitive data housed on its systems. This is apparent, given the number of cyber-attacks over the past several years. Part of the ongoing challenge of safeguarding against such attacks is the fact that an entity is only as strong as its weakest link.

Continuously improving the systematic methodology of identifying, prioritizing and remediating security issues needs to be a state focus. This approach includes:

- Attracting and retaining key security personnel critical for success.
- Leveraging industry defined policies and standards in a template format for evaluating state organizations.

- Executing priority projects swiftly and successfully.
- Investing in tools that amplify the State's ability to detect and prevent security related issues.
- Continuously investing in the training of all business and technical staff, including end users, business owners, system administrators, application developers and network and security administrators.
- Regular testing of applications and system environments to identify risks and immediately define plans for remediation.
- Performing table-top and scenario-based exercises to ensure personnel understand key roles and responsibilities in the event of potential or confirmed security breaches.
- Ensuring the adequate level of cyber-risk insurance is maintained in order to reduce the financial risk to the State in the event of a security breach.

Many states have suffered security breaches over the past several years partly due to the inherent size and complexity of government networks. Arizona has been systematically identifying, prioritizing and remediating security issues over the past three years. One key observation is that this method is an ineffective long-term strategic approach. It lacks the ability to quickly scale and reach the State's approximate 132 agencies, boards and commissions to effectively resolve open risks. In order to properly increase the State's protections, a more aggressive strategy must be implemented.

### **Detailed Analysis**

This detailed analysis contains an example of implementing a single security control in a piece-meal methodology across 80 State agencies, including costs and impact. This arbitrary example utilizes 80 agencies as a framework for discussion. This analysis applies to critical security controls required to

secure protected information. This analysis also applies to other sections of the LSCS Study including Server Utilization, IT Facilities and Cloud Computing.

The State would reduce cost by eliminating redundant systems, improving the management and maintenance of these systems, and leveraging economies of scale during purchase. An example of implementing one security control across multiple agencies is detailed below.

1. On the ADOA website, approximately 132 agencies, boards and commissions are listed.
2. Using one security control, such as Data Loss Prevention (DLP), which typically requires a dedicated server to run the product, could save considerable money when offered as an enterprise service. If 80 agencies were to add DLP to their security controls it would require a purchase of 80 separate servers, 80 people to patch and maintain those servers, and 80 different connection points to the State's infrastructure. These agencies may not have the resources, budget, or the knowledge to implement security controls on their own.
3. Using the same example above, if each of the agencies were to purchase licensing for the DLP product it would require 80 separate purchases through procurement, for potentially 12 different vendor products with different capabilities, and require the vendor to maintain up to 80 different license expiration dates.
4. If DLP were to be standardized into an enterprise service, the State could run the product for all 132 agencies on four servers, requiring one person to patch and maintain the servers, with four connection points to the infrastructure. The State could also perform a single procurement, standardizing on a single product, with one expiration date for the State which meets the business requirements. This would also save money on the bulk purchase of 30,000 licenses versus each agency purchasing 10 to 100 licenses at a time. In addition, DLP capabilities would be provided to all 132 agencies versus only 80 agencies having that capability.

The State would simplify security by implementing a common security strategy and environment.

1. Using the example above with DLP, 80 of the 132 agencies could individually procure different products with different capabilities, from different vendors. The other 52 would not have the capability to protect their data with this security control because they do not have the budget or resources to provide the service.
2. By using competitive procurement processes to standardize selection criteria meeting our business needs, the State could provide a single secure DLP strategy for all 132 agencies.

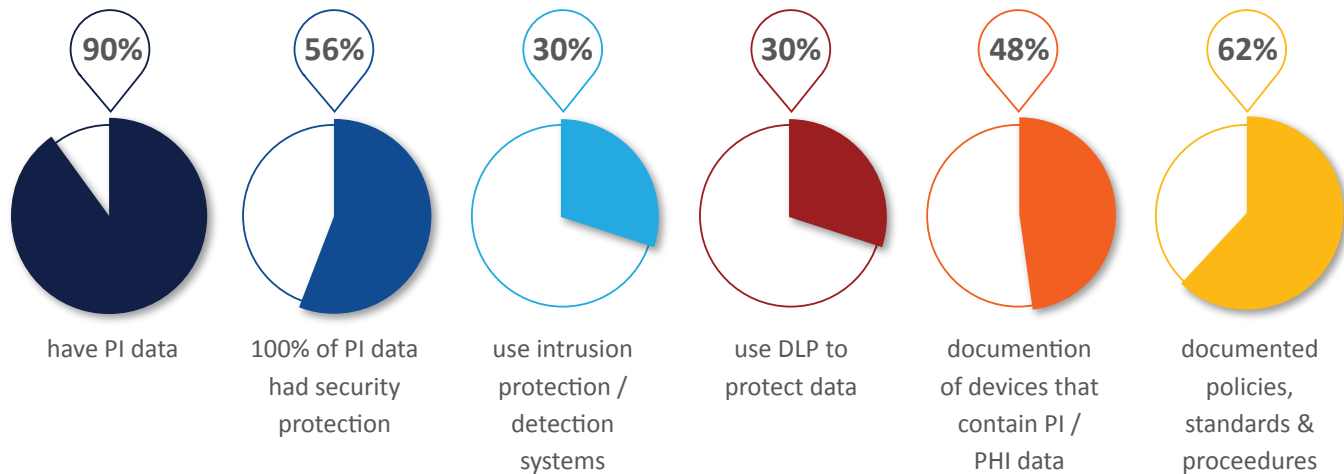
The State would reduce risk by gaining the ability to provide consistent protection to all agencies by establishing a secure framework.

1. Data is regularly exchanged between State agencies. If an agency is unprotected, the shared data could be at risk of malicious or unintended exposure.
2. If a statewide enterprise standard service were utilized, agency resources would be freed-up to focus on the monitoring and mitigation of high risk security threats, as opposed to maintaining DLP services.

The examples listed above are for one security control. As stated earlier, at least twelve security controls can be turned into statewide enterprise services. In addition, virtualization or outsourcing to the Cloud could potentially save additional cost or resources, and the ability to provide better security.

A recent State agency Personal Information (PI) evaluation revealed:

1. 90 percent of agencies claimed to have PI data.
2. 56 percent of agencies reported that 100 percent of their PI data had security protection.
3. 30 percent of the agencies reported using intrusion protection, or intrusion detection systems to protect data.
4. 30 percent of the agencies reported using DLP to protect data.
5. 48 percent of the agencies reported maintaining documentation of all of devices that contain PI or Protected Health Information (PHI) data.
6. 62 percent of the agencies reported having documented policies, standards, and procedures for identification, protection and response to a data breach.



This survey alone shows the State as a whole is incurring significant risk of PI being breached at many state agencies. It also shows many agencies do not have the proper resources to identify security risks and gaps, and are not dedicating sufficient budget resources to the protection of State data.

The State can benefit from taking advantage of statewide buying power to provide an enterprise service for security controls in order for agencies to afford to protect their data. In addition, by providing an enterprise service via enterprise procurement, this opportunity can be extended to other local and county governments.

### **Cost Analysis**

Using the DLP example above, the State of Arizona could potentially save up to \$680,000 in product costs, over three years by offering an enterprise service for DLP, over half of the budget units providing the service individually. Additionally, the State of Arizona could gain up to \$2,180,000 worth of resources to provide other security services for the agencies, boards, and commissions. Finally, an enterprise service for DLP solution would protect all the budget units at a total opportunity cost savings of up to \$2,860,000 over three years. If the State of Arizona could realize these cost savings for each of the twelve enterprise security controls identified, the total cost savings for the State of Arizona could reach \$8.16 million over three years, or an opportunity cost savings of \$34.32 million over three years.

A typical server costs the State of Arizona \$9,000, which includes a three-year support agreement. Each budget unit would require at least one server, and additional servers if some agencies wanted redundancy or disaster recovery.

A typical license cost, on average, would be about \$8 per user per year, which would include maintenance and support. Some of the larger agencies might be able to get the license at \$6, but the smaller agencies would likely pay \$10 - \$15 per user. Many licensing costs are based on quantity or volume, so one purchase of 30,000 licenses would get top savings compared to 80 purchases of 100 licenses or less.



Each budget unit would have to dedicate some resource time to manage and maintain the server environment and the security controls of the product. If it requires 10 percent of a person's time per setup, then that would be 208 hours per year per setup. Managing an enterprise environment is much more efficient by dedicating an entire Full-Time Employee (FTE) worth of time. The average cost rate of an FTE used at the State is \$50 per hour<sup>4</sup> to cover all of the costs associated with the person being physically located in the enterprise. These scenarios are detailed below:

1. A DLP option over three years for 80 agencies, on an individual basis, with 15,000 employees would cost \$3,576,000, and include the following:
  - a. 80 servers at \$9,000 each with three years of maintenance and support
  - b. 15,000 licenses at an average of \$8 per license per year with maintenance and support
  - c. 80 resources spending on average 10 percent of their time (208 hours) per year installing, supporting, patching and maintaining the DLP infrastructure and application at \$50 per hour covering salary, overhead, benefits, and other agency costs
  
2. A DLP statewide enterprise option over three years for all State agencies encompassing approximately 30,000 employees would cost \$708,000, and include the following:
  - a. 4 servers at \$9,000 each with three years of maintenance and support
  - b. 30,000 licenses at an average of \$4 per license per year with maintenance and support
  
  - c. 1 full time resource (2080 hours) per year installing, supporting, patching and maintaining the DLP infrastructure and application at \$50 per hour covering the salary, overhead, benefits, and other agency costs.

<sup>4</sup>[https://gao.az.gov/sites/default/files/APG\\_I\\_B\\_Tax\\_Tables\\_070114.pdf](https://gao.az.gov/sites/default/files/APG_I_B_Tax_Tables_070114.pdf)

- The potential opportunity cost savings for the State of Arizona for a three year period for the enterprise DLP control alone for all agencies and customers is up to \$2.86 million.

The potential opportunity cost savings for the State of Arizona for a three year period for all twelve enterprise security controls is up to \$34.32 million, and the enhanced protection of all agencies and customers.

**Data Loss Prevention (DLP): 80 Separate Implementations**

Resources	Units	Cost/Unit	Hours /Years	Year 1	Year 2	Year 3	Total 3-Year Cost
Servers	80	\$9,000		\$720,000			\$720,000
Licensing	15,000	\$8		\$120,000	\$120,000	\$120,000	\$360,000
Staff*	80	\$50	208	\$832,000	\$832,000	\$832,000	\$2,496,000
<b>Totals</b>				<b>\$1,672,000</b>	<b>\$952,000</b>	<b>\$952,000</b>	<b>\$3,576,000</b>

\*Assumes 10 percent staffing utilization

**Data Loss Prevention (DLP): Statewide Implementation**

Resources	Units	Cost/Unit	Hours /Years	Year 1	Year 2	Year 3	Total 3-Year Cost
Servers	4	\$9,000		\$36,000			\$36,000
Licensing**	30,000	\$8		\$120,000	\$120,000	\$120,000	\$360,000
Staff*	1	\$50	2,080	\$104,000	\$104,000	\$104,000	\$312,000
<b>Totals</b>				<b>\$260,000</b>	<b>\$952,000</b>	<b>\$952,000</b>	<b>\$708,000</b>

\*One full time resource to administrate DLP control

\*\*Assumes discounted unit cost for quantity

<b>Statewide Implementation Savings***</b>	<b>\$2,868,000</b>
--	--------------------

\*\*\*Assumes discounted unit cost for quantity

### **Cyber Risk Insurance**

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify<sup>5</sup> individuals of security breaches involving personally identifiable information. A.R.S. § 44-7501 defines the guidelines for breach notification within Arizona and as it stands today, most state agencies are currently not equipped to provide these type of notifications and maintain compliance with the law in the event of a breach. ADOA has opted to bridge this gap and be compliant with the law by purchasing a cyber-insurance policy that provides first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks. This also includes liability coverage indemnifying the State for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamations well as other benefits including regulatory proceedings, breach expenses, crisis management, notification costs and credit monitoring.

<sup>5</sup><http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

<sup>6</sup>McGrath, Maggie. (2014, January 10). "Target Data Breach Spilled Info on as many as 70 million customers". Retrieved from <http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/>

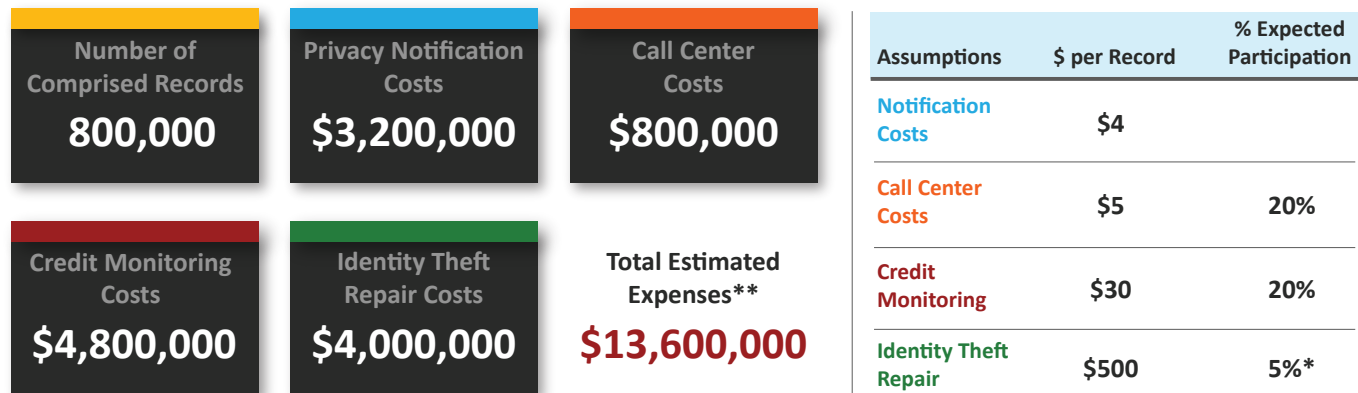
The state has a cyber-insurance policy that protects any entity hosted in the Phoenix State Data Center (SDC), the Tucson Data Center, or the State's cloud offerings, from liability or breach. This policy consists of a pre-negotiated contract with an experienced vendors to offer suitable and reasonably priced services.

### **Privacy Notification Cost Model**

The following table was distributed by Marsh to the State in 2012. Marsh is the current Cyber Risk Insurance provider. This table models the notification costs at \$13,600,000 when only 800,000 records are breached. The estimated assumptions in this model are quite low due to the pre-negotiated contracts. The average cost per record in this model is \$17. Industry standards for notification costs without cyber-insurance normally range from \$100-\$400 for organizations that attempt to do it themselves. Using this model and applying it to Target Store's recent breach of 70<sup>6</sup> million records, it would cost Target \$1.19 billion for notification. Target did have at least \$100 million of cyber-insurance, but that is far short of the estimated notification costs alone.

### Privacy Notification Event Model

Potential value of a privacy event based upon number of records compromised



Marsh Model 2012 - current cyber insurance broker. \*Of monitored experience theft. \*\*Note: Due to variability, does not contemplate forensic, legal and regulatory expense.

Marsh provides a sample event outcome model on their website that shows the probabilities of increasing breach severity<sup>7</sup>.

Event Type	Percentile	Number of Affected Records	Total Cost per Event	
Mean	-	779,741	\$13,454,865	
<b>SEVERITY</b>	1 in 2 Events	50%	5,186	\$340,496
	1 in 4 Events	75%	73,772	\$1,597,941
	1 in 5 Events	80%	143,467	\$2,657,613
	1 in 10 Events	90%	577,148	\$10,914,713
	1 in 20 Events	95%	1,896,416	\$32,442,690
	1 in 100 Events	99%	19,976,225	\$315,257,617

Note: Total cost per event includes both variable and fixed costs.

<sup>7</sup>Marsh USA. (2014, July 7). "Marsh's Cyber-privacy event model: analytics for cyber decision-making". Retrieved from <http://usa.marsh.com/ProductsServices/MarshSolutions/ID/41032/Marshs-Cyber-Privacy-Event-Model-Analytics-for-Cyber-Decision-Making.aspx>

# Mainframe Utilization



In the 2011 study, it was determined that Oklahoma supports seven higher-end mainframe-type systems. The Office of State Finance, Department of Human Services, Office of Juvenile Affairs, Department of Public Safety, Tax Commission, Department of Transportation, and Employment Security Commission support these environments. It was recommended in the report that the State embark on an initiative to combine workloads of mainframe environments within the IT landscape. The strategy includes consolidating mainframe environments into three primary systems initially, and then investigating the adoption of industry trends and eliminate the mainframe environment entirely from its IT landscape. The anticipated savings is more than \$2.5 million in mainframe costs and \$292 thousand in storage for servers and mainframe. It is also anticipated that total infrastructure staffing (mainframe and server) costs will be reduced by more than \$8 million.

In contrast to what has transpired in Oklahoma, Arizona consolidated to three mainframes roughly 10 years ago. The Department of Administration, Department of Economic Security, and the Department of Public Safety support the three environments. Based on current workload, three mainframe systems is the optimal number to provide business continuity and to ensure Department of Public Safety (DPS) security requirements. Arizona has seen the use and dependency of mainframe applications increase significantly over the past two years and has had to invest in replacing two of the three mainframes. The DPS mainframe is relatively small and they are in the approval process for replacing it primarily for continuity reasons.

## Overview

- A. The State currently operates three mainframe computing systems. The DPS and DES mainframes are dedicated to serve the needs of their respective agencies. ADOA operates a mainframe for hosting applications used statewide and hosts applications for eight entities.

- B. Mainframe purchases typically require large, periodic, capital investment and significant, ongoing, operational expense.
- C. Due to increased demand, ADOA-ASET is in the process of leasing a new mainframe. The anticipated annual lease cost will be near \$1,300,000. To accompany the increase in processing capacity of the new mainframe, the software licensing must also be increased. Software licensing costs are based on capacity and utilization. The anticipated mainframe software costs for FY 16 is \$8,525,000. The estimated five-year cost for hardware and software will be in excess of \$52,000,000. Direct staffing to operate the ADOA-ASET mainframe requires more than 40 staff members.
- D. There are 228 applications operating on the three State mainframes of which 77 are assessed by their agencies to be of Low or Medium functional adequacy.
- E. Mainframe resources, particularly programmers, are limited and are expected to be harder to find in the future. The Department of Administration, Department of Corrections and AHCCCS have experienced difficulty recruiting COBOL programmers and both have resorted to using retired programmers who work remotely. This strategy is not sustainable long-term.
- F. The State is in the process of replacing at least three large, critical mainframe applications (the State accounting system, the Arizona Inmate Management System and the Department of Transportation Legacy Platform) with modern solutions capable of operating on distributed computing systems. This approach is in line with the current IT trend of reducing dependence on mainframes and taking advantage of current resource skillsets.

### **Strategy – Manage Capacity, Costs and Resources**

Mainframes are the work horses of the computing world. They have been around for decades and they continue to deliver top of the line performance, but this performance does come at a cost.

Mainframes have enormous capacity, but it is not infinite. ADOA-ASET, whose mainframe has experienced significant growth in workload and capacity over the past two years, is in the process of procuring a new one to meet demand. Monitoring and managing demand is critical to be able to plan far enough ahead to meet business needs. This applies to computing capacity, storage and other aspects of mainframe operations.

As state agencies continue to organically grow, processing demand, costs associated with the increase in demand, increase as well. State agencies should develop multi-year plans that continuously evaluate the operation of these applications on the mainframe. Comparisons should be kept up to date to ensure the right solution is being implemented or to provide cost justification to replace the legacy systems. These plans should be holistic and include hardware, major investment in hosting facilities, and major application rewrites. In some cases it may be beneficial and cost effective to continue to operate the applications in their current form, but this strategy too should be included in a multi-year plan that describes how the applications will be maintained and enhanced over the next seven to ten years.

Colleges are not turning out new mainframe developers and administrators. The State needs to have strategies in place to recruit and retain these valuable resources. The State also needs to have alternate plans for pooling existing resources within the State or contracting for supplemental resources.

### **Detailed Analysis**

Some of the largest computing systems used in Arizona state government are based on mainframe computers. Historically, these systems have been the computing workhorses of business and government for high-volume transaction processing. They typically use applications written in COBOL or other 3rd Generation Language (3GL) or 4th Generation Language (4GL) programming languages such as PL/1, Natural, and CA-Ideal. Note that all further references to COBOL also include these other mainframe programming languages. Industry analysts estimate that between 60 and 80 percent of all business transactions are still accomplished using applications written in COBOL, which was first introduced in

<sup>8</sup>Woodie, H. (2013, March 11).

“If COBOL is too Uncool for school, what’s that make RPG?”. Retrieved from <http://www.itjungle.com/tfh/tfh031113-story02.html>

<sup>9</sup>Mitchell, RL. (2012, May 21).

“Brain Drain: Where Cobol systems go from here”. Retrieved from [http://www.computerworld.com/s/article/9227263/The\\_Cobol\\_Brain\\_Drain](http://www.computerworld.com/s/article/9227263/The_Cobol_Brain_Drain)

<sup>10</sup>Willmott, D. (2012, Aug.

28). “Take advantage of the mainframe talent shortage”. Retrieved from <http://news.dice.com/2012/08/28/mainframe-talent-shortage/>

1959.<sup>8</sup> This is primarily because over the last 50 years large financial and insurance companies developed their own applications on the largest, commercial computers available (mainframes) using COBOL.

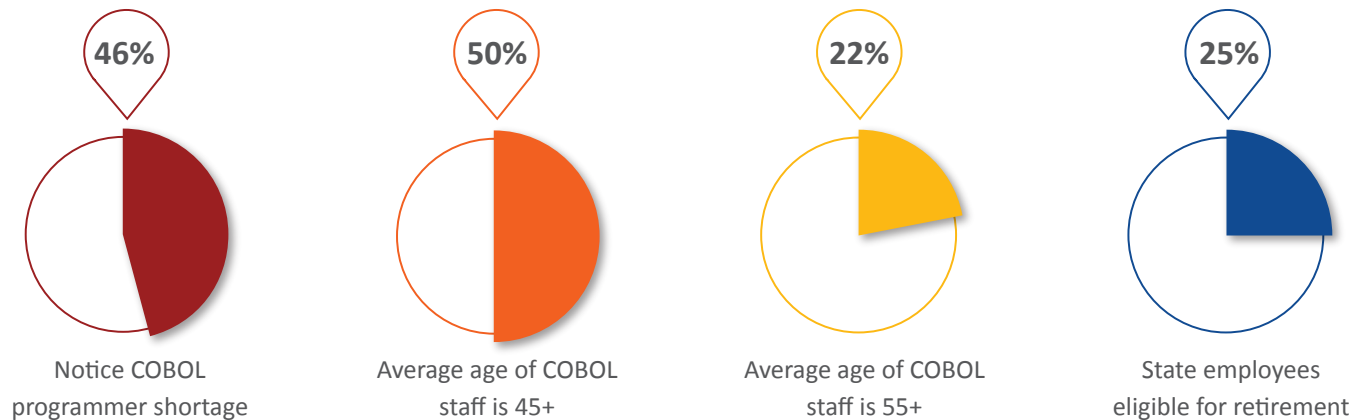
However, over the last two decades, distributed computing, using smaller, mid-range and workgroup servers, has become an available, preferable, and potentially lower-cost alternative to mainframes. The combination of smaller, more powerful servers and modern programming languages also allows organizations to develop internet-ready applications – something COBOL was never intended to do. During this same timeframe, the sources for new mainframe computer systems have narrowed to a single vendor, IBM.

The obvious concerns with mainframe systems are the limited sources for hardware and the costs of hardware. Less obvious, but no less significant, are the outdated programming languages used to develop applications running on these mainframes.<sup>9</sup> Mainframes have evolved such that they include additional capabilities, including the ability to run Linux, Windows, and RISC (Power) applications within the same hardware platform.

Mainframe program languages are no longer being taught in colleges and universities. In some instances where specialized classes have been created to teach COBOL, they were cancelled due to lack of student interest.<sup>10</sup>

In a recent Computerworld survey of 357 IT professionals, 46 percent said they are already noticing a COBOL programmer shortage in the market, 50 percent said the average age of their COBOL staff is 45 or older and 22 percent said the age is 55 or older. Our State agencies are competing for this same diminishing talent pool and must prepare for the fact that statewide 25 percent of the State’s employees are eligible for retirement within the next 5 years. This will likely include some of the State’s mainframe programming and support talent. Retirements, coupled with a high turnover rate (17.3 percent between 2005 and 2010) and wages typically lower than the private sector, will make competing for mainframe talent especially difficult for agencies in upcoming years.





There is also a potential cost for waiting too long before addressing the problem of diminishing talent. It is cheaper and easier to analyze legacy code and migrate the business logic using experienced people who have the institutional knowledge about legacy applications and underlying business processes than it is to try and tackle the problem when they are no longer available.<sup>11</sup>

Discussions about the looming shortage of mainframe programming talent frequently devolve into arguments about the relative value of mainframe programming languages, mainframe applications, or the mainframe hardware itself. The bottom line is that no matter how good the machine, the language, or the program, it takes trained and experienced people to keep these systems running and those people are becoming scarce.

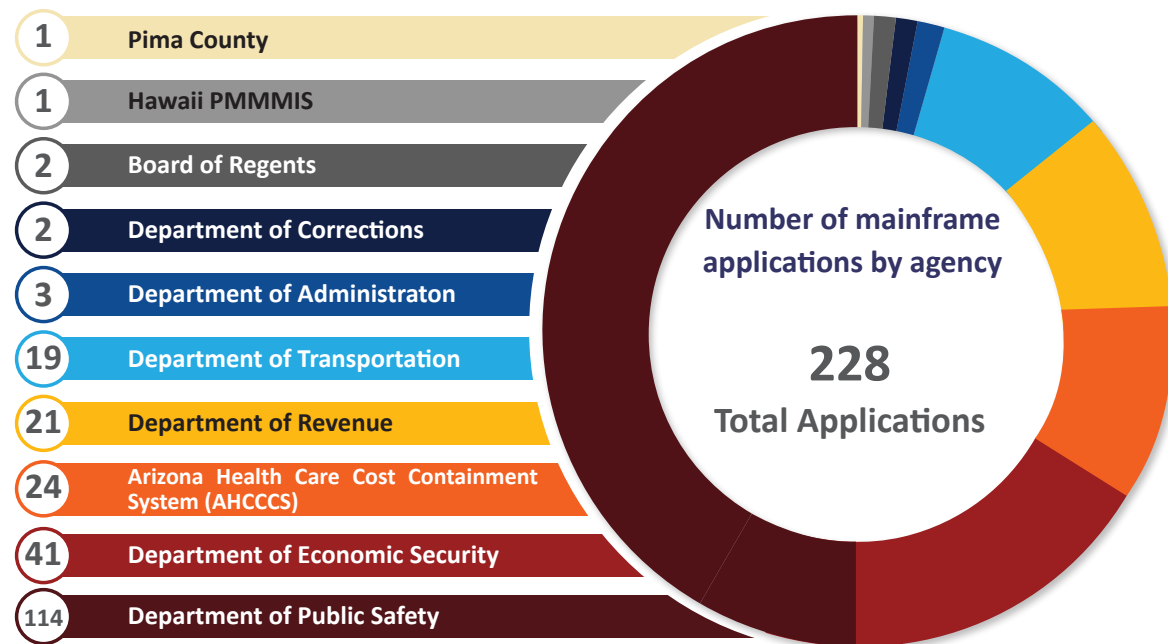
<sup>11</sup>Mitchell, RL. (2012, March 15). "Cobol on the mainframe: Does it have a future?". Retrieved from <http://features.techworld.com/applications/3344704/cobol-on-the-mainframe-does-it-have-a-future/>

### State of Arizona Mainframes and Applications

The State collects IT asset data from 89 of the budget units in the Executive branch of state government. This data was analyzed to determine agencies' reliance on mainframe computing systems. Of the 89 agencies, the data shows that 8 agencies have programs that operate on a mainframe. A total of 228 mainframe applications were reported for the entire state this year, whereas the peak number in 2007 was 269.

The data indicates that the agencies with the largest number of mainframe applications are the Department of Public Safety with approximately 81 mainframe applications, and the Department of Economic Security with approximately 41 mainframe applications.

The Department of Administration also operates a mainframe for use by subscribing agencies and currently hosts 73 applications for the following agencies: AHCCCS (24 applications), the Department of Transportation (19 applications), the Department of Revenue (21 applications), the Department of Administration (3 applications), and the Department of Corrections (2 applications). There are also two external entities, the State of Hawaii and Pima County, that have applications hosted on the ADOA mainframe. Two of the Department of Administration applications are operated for statewide access or benefit. They include the State financial system (AFIS), and the State employee benefits and insurance system (BITS).



### **ADOA Mainframe Operations**

The value of any computing system, be it a mainframe, server, or even a desktop, is substantially based on how well the system performs the computing tasks it was provisioned to perform and the cost of performing those tasks.

ADOA purchased their current mainframe in 2010 for \$2,111,407. Peripherals for data storage, tape backup, etc. increased the total purchase cost to \$2,862,901. Annual maintenance on this system is \$461,426 and the annual software cost is \$4,494,839 (does not include the cost of State-developed applications). Operating the mainframe requires more than 40 direct staff members. The ADOA billing records for the last full year show approximately \$23,000,000 per year for mainframe-related services billed to subscribing agencies.

Mainframe utilization has significantly increased over the past two years and the ADOA mainframe has reached capacity. To provide the most flexibility and to avoid federally disallowed costs, the State is in the processes of leasing a new higher capacity mainframe. This new mainframe should be in place in October or November of 2014. The approved implementation cost is \$2,900,000. The annual lease cost will be \$1,300,000. To accompany the increase in processing capacity of the new mainframe, the software licensing must also be increased. Software licensing costs are based on capacity and utilization. The anticipated total mainframe software cost for FY 16 is \$8,525,000. The estimated five-year cost for hardware and software will be in excess of \$52,000,000.

ADOA-ASET is currently evaluating the mainframe storage capacity, utilization and demand. In FY 13, ADOA-ASET had forecasted enough storage capacity to meet customer needs until the end of FY 16. Given the increased demand and processing capacity utilization, ADOA-ASET believes this timeline will shrink.

### **Alternatives**

There are several alternatives that have been evaluated, but there is no single solution that fits all of the State's unique requirements. Among the available alternatives are mainframe outsourcing, application outsourcing, and application migration. Each will be discussed and relevant case studies or articles referenced to demonstrate experiences for other states and organizations.

### **Mainframe Outsourcing**

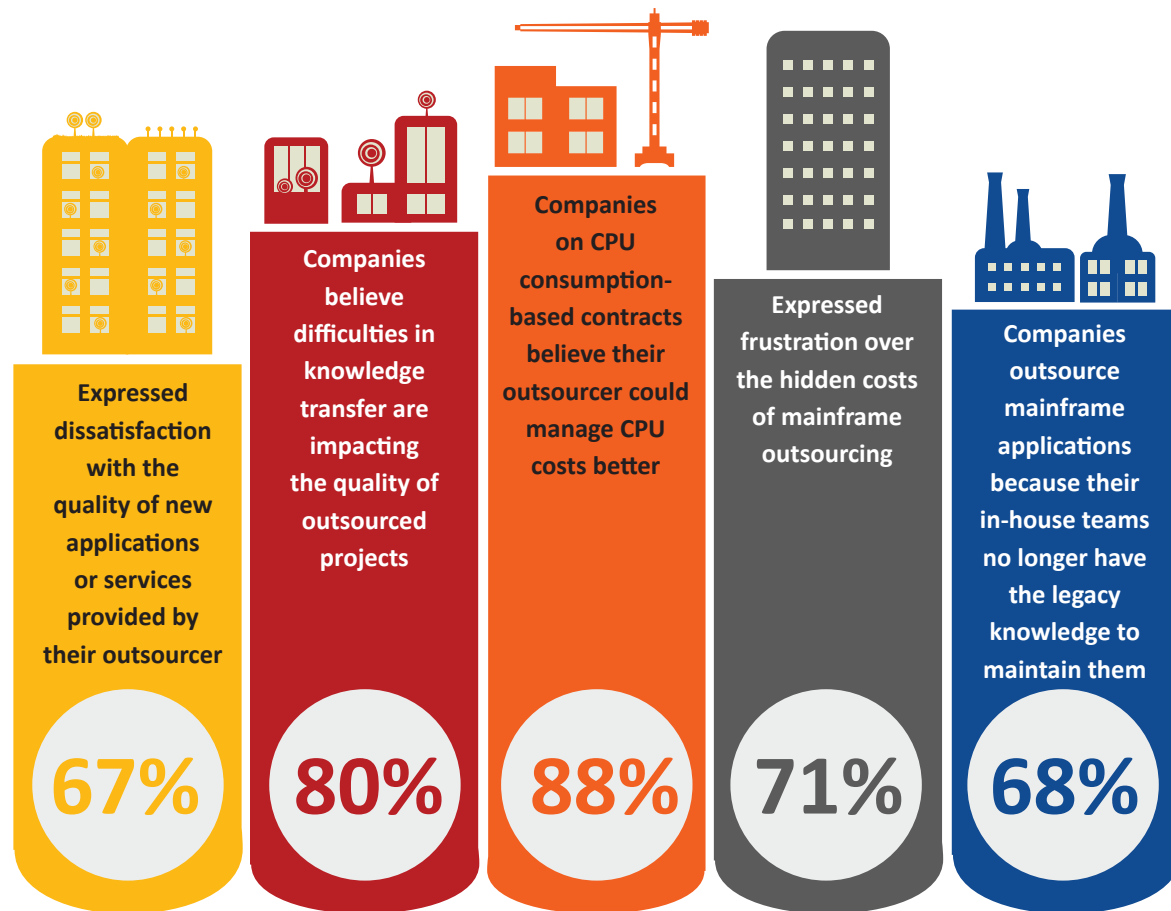
Mainframe outsourcing typically involves contracting with a commercial company to supply mainframe hardware, the operating system, and technical support services in their facility. These arrangements also usually include data storage, tape backup and offsite storage, and disaster recovery services. Less common arrangements can include hosting one's mainframe in a commercial data center or retaining one's equipment but having it remotely maintained by a commercial company. Vendors for mainframe outsourcing advertise 20 to 40 percent possible savings over owning one's own mainframe.

### **Mainframe Application Outsourcing**

Similar to outsourcing of the hardware, many organizations have outsourced the development of their applications to the same companies that host them or to other commercial application development companies. Perceived cost savings is the primary motivation for outsourcing mainframe application development and/or support; however, lack of available internal skills is also a driver.

In a 2012 Compuware study performed by Vanson Bourne, 520 CIOs of enterprise organizations were queried on their experiences with mainframe outsourcers. Some key findings are presented in the digram below:<sup>12</sup>

<sup>12</sup>Feravich, S. (2013, July 22). "Mainframe outsourcing: Removing the hidden costs". Retrieved from <http://enterprisesystemsmedia.com/article/mainframe-outsourcing-removing-the-hidden-costs>



### Application Migration

Mainframe application migration, often called re-platforming, entails using a programming language compiler to recompile existing mainframe source code and redeploy the applications onto a different operating environment. In this process, there is typically no attempt to make changes to the code except to apply only the modifications necessary for the application to execute properly in the new environment.

<sup>13</sup>Exodus Project – Pigs Really Do Fly (2012, August 31). Retrieved from <http://publicsafety.ohio.gov/links/Exodus%20Case%20Study%20-%20Ohio%20Department%20of%20Public%20Safety%20August%202012.pdf>

<sup>14</sup>[http://www.fujitsu.com/us/casestudies/fc\\_case\\_WashingtonState.html](http://www.fujitsu.com/us/casestudies/fc_case_WashingtonState.html)

<sup>15</sup><http://download.microsoft.com/download/8/7/6/8762c1b0-e1e9-48f5-8e57-aa8d508acb6a/Washington%20State%20Department%20of%20Licensing%20Case%20Study.doc>

### **Case Study: Ohio**

The Ohio Department of Public Safety undertook a project to migrate their COBOL applications from an end-of-life Unisys mainframe onto a Windows server environment. The project took five years, required 84,500 hours of staff time to complete, and is expected to save \$7 to \$10 million over the upcoming five years.

Of interest in this case is that 84,500 hours equates to over \$4.2 million in staff expenses for the five-year project (assuming 84,500 at \$50 per hour). For the duration of the project, other important projects went unsatisfied or were significantly delayed. This five-year migration project was considered successful in that they were ultimately able to operate on less expensive, supportable hardware. However, they are still operating and maintaining the same legacy COBOL applications with all of the inherent risks and shortcomings detailed above.<sup>13</sup>

### **Migration Case Study: Washington Department of Licensing<sup>14</sup>**

The State of Washington Department of Licensing (DOL) maintains more than 20 million driver, vehicle, and vessel records, and provides services to businesses, law enforcement agencies, and citizens. The department's mainframe software was consuming ever-increasing resources in workarounds and maintenance. The DOL worked with its partner, Fujitsu Consulting, to move the agency's data to Microsoft® SQL Server 2000 Enterprise Edition running on Windows Server 2003 Enterprise Edition, with Internet Information Services (IIS) 6.0. The agency's COBOL applications were migrated to the Microsoft .NET Framework and tied together with scripts written in Microsoft Visual Basic .NET 2003. The migration modernized the agency's data system yet took advantage of current business processes. The DOL expects to save \$1.2 million per year in IT maintenance costs and to free up 3,000 hours of IT staff time.<sup>15</sup>

### **Outsourcing**

Several states have chosen to outsource all or large portions of their computing infrastructure in order to consolidate responsibilities and achieve cost savings.

<sup>16</sup>Overby, S. (2010, August 4) "Don't mess with Texas: 7 lessons from state IT outsourcing disasters". Retrieved from [http://www.cio.com/article/602072/Don\\_t\\_Mess\\_with\\_Texas\\_7\\_Lessons\\_From\\_State\\_IT\\_Outsourcing\\_Disasters](http://www.cio.com/article/602072/Don_t_Mess_with_Texas_7_Lessons_From_State_IT_Outsourcing_Disasters)

<sup>17</sup>Opsahl, A. (2010, May 13). "IBM and Indiana suing each other over cancelled outsourcing deal". Retrieved from <http://www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html>

<sup>18</sup>Wood, C. (2012, July 19). "Nobody wins in Indiana vs. IBM lawsuit, judge says". Retrieved from <http://www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html>

<sup>19</sup><http://data-informed.com/oklahoma-it-consolidation-sets-stage-for-analytics-use-cases/>

The examples from Indiana and Oklahoma below illustrate the substantial financial and reputational risk confronting states that undertake large-scale consolidation or modernization when they rely primarily on outsourced vendors. Virginia and Texas both intended to reduce costs, improve services, simplify their computing environments, and improve their disaster recovery posture. Both states presumably followed their respective state's selection and contracting process to engage large, reputable vendors to complete their projects. Both ended up taking longer than expected, spending more than expected, and resulted in contractual disputes.<sup>16</sup>

### **Case Study: Indiana**

In another case of large-scale outsourcing, the State of Indiana awarded a ten-year \$1.6 billion contract to streamline its welfare eligibility system. In late 2009, the Governor stopped the work on the system he characterized as "unworkable" because of high error rates and slow processing of eligibility requests. Indiana sued for the \$437 million they expended on the project and the vendor countersued for damages. Neither party prevailed, however the vendor was awarded \$12 million for hardware that Indiana continued to use.<sup>17, 18</sup>

## **Mainframe Consolidation**

### **Case Study: Oklahoma**

The State of Oklahoma's ongoing IT consolidation project, designed to save money on data center operations and staff, also set the stage for an iterative, analytics-driven strategy to use data in new ways to save on service delivery and inform policy decisions, according to State CIO Alex Pettit.<sup>19</sup>

Implementation of the strategy took a step forward on April 9, 2013 when Oklahoma and IBM reported work on a data center consolidation project that was expected to save \$13 million over the next five years by retiring five old mainframes and transferring the processing work they do to one IBM System z mainframe.

### **Recent and Current Efforts in Arizona**

There are several significant initiatives related to mainframes and mainframe applications underway in the State. In 2012, the Arizona Department of Administration received approval and funding to replace the statewide Arizona Financial Information System (AFIS). The Arizona Department of Corrections received approval in August 2013 to proceed with a multi-year project to replace the Adult Inmate Management System (AIMS).

### **Arizona Department of Administration (ADOA) – Arizona Financial Information System (AFIS) Replacement**

The State currently uses a system developed by KPMG LLP in the 1980s (R\*STARS) as its statewide accounting system, referred to as the Arizona Financial Information System (AFIS). This system was installed at the State of Arizona in 1992 and resides on the ADOA mainframe. AFIS is used by virtually all State agencies; however, the three State universities have their own financial management systems and generate payments from those systems. At this time, replacing the universities' systems is not considered part of this project.

Three large agencies, the Arizona Department of Transportation (ADOT), the Arizona Department of Economic Security (DES) and the Arizona Health Care Cost Containment System (AHCCCS), have their own internal financial management systems that are interfaced with AFIS. The systems at DES are reaching the end of their expected useful lives and are in need of replacement. ADOT no longer obtains support from its financial software vendor and will require investment of additional funds to maintain the system in coming years.

According to ADOA leadership, the State's accounting systems do not provide the necessary management information required for Arizona to be a responsive state government. They do not provide a platform for optimizing business operations; they do little more than simply record transactions. The desired approach is to replace AFIS and the financial systems maintained by ADOT, DES, AHCCCS, and other agencies as appropriate, in a cost-effective and strategic manner. The replacement of AFIS and other major financial



reporting systems also provides the opportunity to review the financial business functions of the State and apply (as appropriate) business-process best practices that are currently used by the public and private sectors. The desired outcomes are streamlined decision-making, reduction in risks associated with obsolete administrative systems, and more responsive government. The replacement will eliminate the substantial risk of failure associated with AFIS. It will achieve business process standardization based on best practices, economies of scale, and efficiency gains through the implementation of a single, unified platform for all state agencies. It resolves much of the fragmentation associated with the State's existing administrative systems environment, and will enable more efficient processing and eliminate redundant data entry and reconciliation tasks. It will eliminate funding requests for agency-specific ERP systems and reduce future requests for other administrative supplemental or shadow systems as agency needs are more fully met by the statewide ERP system.

### **Arizona Department of Corrections (ADC) – Adult Inmate Management System (AIMS) Replacement**

The Adult Inmate Management System (AIMS) is built on a CICS/COBOL (1978) programming platform. This programming platform is outdated and most public and private IT organizations have been moving away from CICS/COBOL based systems to newer technology platforms. ADC has had limited success in finding, recruiting, hiring and retaining programmers with CICS and COBOL experience. There are currently no schools offering these mainframe-based programming skills in the State of Arizona. Risk continues to escalate as internal COBOL programmers retire and the pool of potential candidates shrinks. ADC has recently been successful filling two positions with retirees; however, this pool is shrinking as well.

The calculations used to determine inmate release dates are not always accurate and there are certain types of calculations that must be completed manually due to system limitations. The AIMS algorithm for sentence calculations is complex. The code spans three major areas of law, with additional complexity due to the overall sentencing structure. ADC dependence on AIMS limits its ability to keep up with inmate movement and changes, release calculations, criminal code changes and interfacing with other applications or agencies. Further, each prison must maintain a duplicate paper record on each inmate since AIMS does not have the ability to import the information from court documents, pre-sentence

and disciplinary reports, or provide prior felony conviction packets to prosecutors. Information placed in AIMS requires manual sentence verification prior to an inmate's release.

ADC requested \$8,000,000 (\$24,000,000 over three years) to replace the current AIMS program with a modern adaptable platform for inmate management. This new system will tie into the agency's existing computing infrastructure and will be based as closely as possible on a commercial off-the-shelf (COTS) deployment. This deployment will enhance data entry accuracy, real-time reporting, reduce maintenance for programming support and will be in compliance with statewide Enterprise Architecture computing requirements. When fully implemented, the AIMS replacement program will eliminate the cost associated with manual record keeping and the current requirement to maintain duplicate files.<sup>20</sup>

#### **Arizona Department of Child Safety (DCS) – CHILDS System Replacement**

*“DCS (formerly DES) uses a software program called CHILDS to track all reports and cases at CPS. The program documents the status, demographic characteristics, location and goal for every child who is in the Department's care. CHILDS tracks reports that are made through the hotline, initial assessment and investigation of reports, case management, adoption, eligibility determination, staff management, provider management and payment processing, among other services.*

*The software system was implemented in the 1990s as a client-server system and is unable to be used on mobile devices or accessed online from remote locations. Additionally, CHILDS is a very cumbersome system and reduces caseworker efficiency.*

*The Executive Branch recommends a \$10 million appropriation to DCS for the initial implementation of a full system replacement of CHILDS. At the moment, DCS is assessing the specific cost, exact system requirements and required features, and a final cost estimate had not been received at the time the Executive Budget Recommendation was finalized.*

*The Executive recommends an additional \$15 million in both FY 2016 and FY 2017 to continue implementation of the CHILDS replacement.”<sup>21</sup>*

<sup>20</sup>2013 Project Investment  
Justification

<sup>21</sup>State of Arizona – The Executive  
Budget – Fiscal Year 2015 (2014,  
January). Retrieved from [http://  
www.azgovernor.gov/documents/  
AZBudget/FY2015/FY2015\\_  
ExecBudget\\_SummaryBook.pdf](http://www.azgovernor.gov/documents/AZBudget/FY2015/FY2015_ExecBudget_SummaryBook.pdf)

This information was pulled from the DES strategic plan. With the creation of the new DCS agency, plans are being evaluated to ensure that the previous approach meets the updated needs of the department.

**Arizona Health Care Cost Containment System (AHCCCS) – PMMIS Performance is Degrading, Need to Explore Options for Replacement**

*“The AHCCCS Information Systems Division (ISD) must be ever vigilant regarding security of our systems and information. As AHCCCS grows, developing and implementing new systems and more technology, we are faced with new security threats that have to be addressed. Security policies must be developed and maintained that meet growing state and federal requirements, and ISD staff are required to make more effort than ever before just to stay at the same threat level. The AHCCCS ISD is responsible for providing technical support to the Hawaii Medicaid program, which means ISD staff must also maintain the security of Hawaii’s information as well. In addition to the AHCCCS mainframe (PMMIS), ISD will continue to keep non-mainframe systems and applications running consistently and efficiently. This includes server based applications, network infrastructure, the data warehouse, and bandwidth for communication. It is important to note that PMMIS is a very mature system. Although it is still functional, performance is slowly degrading over time and maintenance of the mainframe is becoming more challenging. AHCCCS will need to begin to explore options for replacing the mainframe application in the near future, as replacement is the long-term solution.”<sup>22</sup>*

**Department of Public Safety (DPS)**

The agency currently relies on increasingly outdated information systems.

*“The agency currently relies on increasingly outdated information systems for both internal functions and external links with criminal justice agencies. Changing technology and interoperability requirements have made DPS communications systems obsolete.*

<sup>22</sup>AHCCCS Strategic Plan – State fiscal years 2014-2018, (2013, June). Retrieved from [http://www.azahcccs.gov/shared/Downloads/StrategicPlan\\_14-18.pdf](http://www.azahcccs.gov/shared/Downloads/StrategicPlan_14-18.pdf)

*Many of the DPS information systems consist of mainframe-based technology. The most essential of these systems must be supplemented or replaced to be compatible with new technology using database management, browsers, internet, intranet, and extranet solutions for performing processes. The need for components that can eventually be part of a comprehensive records management program is critical to meeting mandates, legal requirements, and public information expectations. Application of newer technologies will increase efficiency internally, as well as allow the agency to better serve the State's criminal justice efforts.*

*The Department also operates the Arizona Criminal Justice Information System (ACJIS) which links crime information centers in Arizona to other states and the national system operated by the Federal Bureau of Investigation (FBI). In recent years, the FBI implemented technological upgrades to enhance the exchange of criminal information and improve criminal record processing. DPS must continue replacing outdated technology used on the State network to enable Arizona agencies to take advantage of the federal enhancements which extend modern crime fighting tools to officers in the field.”<sup>23</sup>*

<sup>23</sup>Department of Public Safety  
Strategic Plan – Fiscal Year 2014,  
(2013, September 10). Retrieved  
from [http://www.azdps.gov/  
About/Reports/docs/AZDPS2014.  
pdf](http://www.azdps.gov/About/Reports/docs/AZDPS2014.pdf)

# Server Utilization



Server consolidation was another recommendation as part of the 2011 Oklahoma study. The goal of server consolidation is to utilize more efficient computer server resources in order to reduce the overall number of required servers. The study determined Oklahoma had approximately 2,200 servers supporting its operations. In addition, it recommended that the State target 1,540 of these servers as candidates for virtualization over the next five years. Lastly, it recommended the State should consider adopting a “virtual first” policy for all new installs.

Arizona has reduced its server footprint by 26 percent since 2011. Between 2011 and 2014, Arizona’s number of operational servers was reduced from 3,463 to 2,576 due to virtualization and migration to cloud services. Arizona has realized an estimated ongoing operational support cost avoidance of approximately \$8.87 million annually, or \$44.35 million over a five-year period.

## Overview

- A. 61 of the State budget units in the Executive Branch operate approximately 2,576 servers.
- B. The total reported initial cost of all servers in the State is approximately \$26,450,000.
- C. The useful life of a server is typically five years. This means that ideally servers are refreshed (re-purchased) every five years. However 1,354 of our servers (53 percent) are already over 5 years old. Approximately 35 percent, or 893 of the State’s servers, are 7 or more years old.
- D. Industry standards indicate that typical utilization of a standalone, physical server is 10-25 percent. The remaining 75-90 percent of unutilized capacity cannot easily be made available to other applications or agencies for technical, security and policy reasons.

- E. The estimated purchase cost of a typical two-processor server is \$12,000. The costs of large mid-range servers and clusters of servers can exceed \$250,000.
- F. The estimated annual ownership cost of a typical server is \$10,000.
- G. The State should anticipate direct ownership costs of approximately \$25,760,000 per year related to the current number of servers owned by the State. Approximately \$6,180,000 per year will be required to refresh existing servers at the rate of 1/5 per year.
- H. At the time of purchase, most state agencies do not have budgeting provision for anticipated server refreshes.
- I. Each server is a potential security vulnerability point. The risk is greater with older equipment and operating systems, including the less than diligent security and patch management. Due to the age of some of the State's servers, they may be running unsupported operating systems.
- J. The acquisition and administration of these servers is performed at the agency level to fulfill the mission of each acquiring agency. Likewise, security, risk management, and disaster recovery are the independent responsibilities and costs of 63 individual budget units.
- K. Industry analysts conservatively estimate that a single system administrator can manage 40 physical servers. Forty-four agencies report owning less than 40 servers in 2014.
- L. Each agency that operates its own servers must also maintain a hosting facility with appropriate physical and electronic security, temperature control, power protection and cabling.

### **Strategy – Move from Physical to Virtual or Cloud and Reduce Cost and Risk**

Servers are necessary infrastructure to run operations for nearly every state agency. They provide core back-office capabilities such as file storage, network domain administration, printer management, data base, virtual private network and many other capabilities. Servers are also used as platforms for running business applications such as email, accounting, document management, web applications, application servers, customer relationship management and thousands of other systems. Servers can run standalone, clustered or virtualized into large-scale complex systems.

State agencies continue to replace physical servers and move to virtual computing platforms wherever it appropriate. This strategy has many benefits including:

- Reduced administration by providing centralized management tools and additional features like snapshots and cloning capabilities
- Decreased maintenance, upgrades and support
- Increased energy efficiency, which reduces power and cooling needs
- Reduced overall data center footprint (space necessary for servers)

While moving to virtual servers can reduce the overall number of system administrators required to manage the sheer number of physical servers, it also increases the skills required to take advantage of the more robust solution. Developing detailed processes for automating virtualization, sophisticated monitoring tools and ensuring systems are patched and secure requires new and additional skills.

The State provides a shared services infrastructure that is secured, optimally virtualized, and scalable for many state agencies today. ADOA-ASET is constantly working with agencies to evaluate which systems can be virtualized, moved to cloud services or need to remain on-premise.

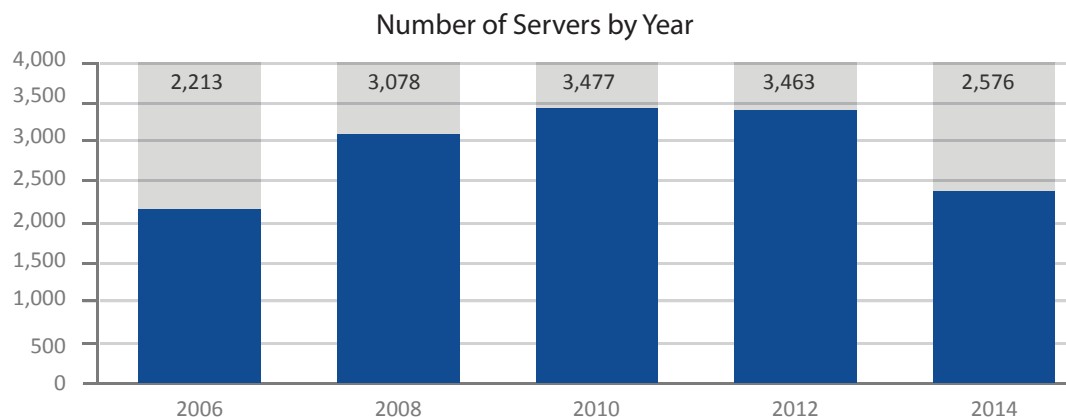
Virtualization and centralization are not always the optimal solutions. Some legacy applications cannot be moved into virtualized environments. There may also be regulatory or legal barriers for combining systems. Application performance is another major factor that must be considered. Replacing or

refreshing applications, migrating environments and scaling virtualization infrastructure also comes with an upfront investment cost. Timing, server refresh cycles, software license renewals and the disposition of existing servers and associated hardware are also factors. Further study is necessary to understand implementation costs, total cost of ownership, security, anticipated savings and Return-on-Investment (ROI).

Leveraging cloud capabilities is quickly overtaking on-premise physical and virtual servers. Cloud computing capabilities are covered in another section of this report.

### Detailed Analysis

From the IT Inventory data, the 89 Budget Units report a total of 2,576<sup>24</sup> servers. It is probable that this number is understated since many of these units were purchased as clusters or systems containing as many as 30 servers while reported under a single asset control number. Using the reported numbers, the State experienced a 58 percent increase in the number of servers between the years 2006 and 2011. In the ensuing years, this number has dropped significantly to the current 2,576. This 26 percent drop in the total number of servers since the peak in 2011 can be largely attributed to server virtualization as well as the moving of capabilities to cloud services. Several of the larger agencies confirmed that they are using more powerful servers, server virtualization and cloud capabilities.



<sup>24</sup>IT Inventory: 2014 Server count by agency



The total acquisition cost of the State's 2,576 servers as reported in the IT Inventory data is approximately \$26,450,000.<sup>25</sup>

### Server Cost Analysis

As one would expect, the larger agencies have a greater number of servers; Department of Transportation reports 443, Department of Public Safety 254, Department of Administration 240, and the Department of Corrections 173. Fourteen agencies account for 80 percent of the total. At the other end of the spectrum, 44 agencies reported owning 40 or fewer servers for a total of 432 servers. Of these, 30 agencies reported owning less than 10 servers each.

A 2007 article on the business value of server virtualization estimated the annual cost of a data center server at \$9,000.<sup>26</sup> Using this rule of thumb and allowing for inflation, it is fair to place the annual direct ownership cost of a typical server today at around \$10,000.

The State reduced the total number of servers in 2012 from 3,463 to 2,576 in 2014. This reduction of 887 servers (26 percent) yields a cost avoidance value of \$8,870,000 annually or potentially \$44,350,000 over a five year period. This is a positive indicator for operational excellence and additional initiatives should be continued. The cost of continuing to operate the 432 servers owned by the smallest 44 agencies is more than \$4,300,000 annually and presents an opportunity for the State to identify additional cost savings.

Any agency that operates their own server or group of servers must necessarily perform or contract for an appropriate level of server administration, maintenance and security. These responsibilities include data backup, disaster recovery planning, classification of data and high risk assets, security compliance, system monitoring, log management, incident response planning and management, account and access management, configuration management, change management, performance management, patching and updates. These are specialized tasks that should be performed to control risks and minimize operational disruptions. These best practice frameworks include: COBIT (Control Objectives for Information and

<sup>25</sup>IT Inventory: 2014 Cost of Active Assets by Agency. Includes 2012 assets for agencies not reporting in 2014

<sup>26</sup>Pisello, Tom. (2007, September 4). "The business value of server virtualization". Retrieved from <http://blog.alinean.com/2007/09/business-value-of-server-virtualization.html>

Related Technology); ISO (International Organization for Standardization); ITIL (Information Technology Infrastructure Library); NIST (National Institute of Science and Technology); HIPAA (Health Insurance Portability and Accountability); FERPA (Family Educational Rights and Privacy Act); IRS Publication 1075 and Payment Card Industry (PCI).

Large IT operations justify the expense of skilled specialized staff to perform these functions. Some examples cite a single administrator managing more than 100 physical servers; in other examples the number is as low as 15 depending on how homogenous the operating environment. The ratio used in the example above and elsewhere in our research indicates that 40 physical servers per administrator is a reasonable expectation.

Much like the mainframe, servers can be partitioned (virtualized) to create several virtual servers on a single physical machine. Virtualization takes advantage of underutilized processor and memory capacity available on modern, multi-core servers allowing them to host multiple applications simultaneously, each in their own operating environment. This process is even more beneficial when larger groups or clusters of servers are virtualized allowing applications to be installed on more than one physical machine to provide inherent redundancy. Agencies that operate small numbers of servers are generally not able to implement server virtualization due to the cost of the hypervisor software and specialized administration skills required.

Industry estimates indicate that the resources of physical servers are typically only tasked at approximately 10 to 25 percent of their capabilities. A 2011 article from StateTech magazine provides two examples of local governments that reduced their physical server counts from 28 to 4 and from 30 to 6 respectively, using server virtualization. In addition to reduced server costs, the examples also highlight other advantages of virtualization including lower power and cooling cost, faster server provisioning and improved disaster recovery<sup>27</sup>. Continuing the example, using these ratios, the 437 servers operated by the smallest agencies can be reduced to about 80.

<sup>27</sup>Stein, E. (2011, Jan. 11). "Server Sense". Retrieved from <http://www.statetechmagazine.com/article/2011/01/server-sense>

Those same 432 servers currently occupy up to 275 racks. Consolidating them to a single data center in about 3 racks may free up as much as 8,000 sq. ft. of floor space in those 44 agencies. Some infrastructure may be necessary within the agencies. Additional planning is necessary.

### **ADOA-ASET Shared Computing Services**

While developing this report, ADOA-ASET evaluated its existing physical and virtual infrastructure used to deliver shared services for state agencies. ADOA-ASET has created a detailed strategy and roadmap to convert physical servers to virtual, move servers and capabilities to the cloud or sunset servers completely. This roadmap is planned to execute through October 2015.

ADOA-ASET plans to reduce the total server count by 34 percent, or from 240 (physical and virtual) servers to 158. ADOA-ASET will reduce the total physical server count from 85 to 26. Sixteen servers will move to the cloud and 43 servers will be sunsetted. Of the existing 155 virtual servers, ADOA-ASET plans to move 90 to the cloud, sunset 39 and retain 26 within the State Data Center (SDC). ADOA-ASET is still working through the assessment of disaster recovery and business continuity requirements with state agencies. Additionally, ADOA-ASET is working with more agencies to provide computing services and anticipates this plan will continue to change. ADOA-ASET also intends to share this methodology with other agencies to perform this same level of assessment.



Just prior to the Oklahoma report being published in 2011, the State of Oklahoma completed the construction of a multi-million dollar data center. The total cost of the construction was not provided in the final report. As part of their cost saving infrastructure initiatives, Oklahoma plans to consolidate 30 data centers down to three, which should allow them to realize cost savings by eliminating rent and other overhead costs. While they anticipate less than \$1 million in cost savings from data center consolidation, they expect this initiative to lead to other savings as a result of staff reduction and application consolidation.

In comparison, Arizona has 28 data centers, one of which is the centralized State Data Center (SDC). Arizona had major issues with the SDC since 2011 and has invested several million to stabilize the environment. The SDC is not an ideal facility and will require millions more to reach optimized operations. Many of the other data centers in the State have similar issues. Alternately, Arizona has opted to contract with the private sector to provide data center services. The Department of Economic Services is working to take advantage of this new strategy. Due to current rent policies in Arizona, it could be hard to realize some of the cost savings from shutting down other data center facilities.

## Overview

- A. The State IT Facilities survey identified 28 data centers, 57 server rooms, and 7,500 additional square feet of designated IT equipment spaces located in office areas within state agency facilities.
- B. IT facilities are significantly more expensive to own and operate than general office space. They require power conditioning, backup power, fire suppression, air conditioning and physical security.
- C. Servers are mounted in server racks. The average server rack usage in this state's datacenters and server rooms is only 63 percent (37 percent of available rack space is unused statewide). Maintaining underutilized capacity in any number of IT facilities is costly and inefficient.

- D. Managing IT facilities is not a core business function of most state agencies.
- E. The State has invested over \$5.2 million in IT facilities and critical infrastructure over the past three years to improve the continuity and disaster recovery capabilities of the State Data Center (SDC).
- F. In September of 2014, the State awarded a statewide contract for an alternative data center. Over the next two years DES plans to move their systems into this new data center.

**Strategy – Assess Existing IT Facilities; Justify Continuity or Remediation**

Arizona has made significant investment in the State Data Center (SDC) over the past three years. As referenced in the Overview above, more than \$5.2 million has been invested into power, network, storage, and large-scale computing. These improvements have dramatically stabilized the SDC. However, several million dollars more are necessary over the next few years to adequately address generator power, diesel fuel capacity, fire suppression issues, plumbing problems, sufficient monitoring capabilities, physical security and ongoing maintenance deficiencies.

Addressing these same issues for all 85 data centers and server rooms may be unrealistic at this point.

In September 2014 the State awarded a statewide contract for an alternative data center.

State agencies should continue to conduct detailed data centers or server rooms risk assessments for the purpose of developing business plans to address critical risks. Ongoing maintenance also needs to be part of these evaluations. In their business plans, BUs should consider critical upgrades, leveraging the SDC, moving to the new alternative data center, moving to the cloud or outsourcing.

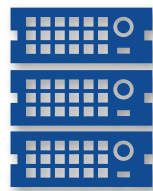
Cyber security should also be considered by the BUs. Assessments should include detailed cyber security assessments based on the 17 statewide security/privacy policies and the more than 200 controls for protected information. The State provides multiple cyber controls at the statewide level through AZNet,

but the majority of the controls need to be applied at the data center, infrastructure or application level for each data center or server room.

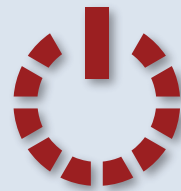
### Detailed Analysis

Data centers and computer room facilities are far more expensive to build, own, and operate than ordinary real estate. In March 2014, 89 state agencies, boards, and commissions were surveyed to gain a better understanding of the number, type, and condition of IT equipment facilities the State operates. This information is relevant to the cost of computing systems as each facility incurs operating costs, requires maintenance and upgrades, and presents a set of risks and vulnerabilities for systems and data.

For the purposes of the survey, a data center was defined as a dedicated facility with the following attributes:



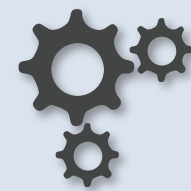
Physically houses IT equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches, routers, data storage devices, load balancers, wire cages or closets, vaults, racks, and related equipment.



Has dedicated power, cooling, and fire suppression systems.



Stores, manages, processes, and exchanges digital data and information.



Provides application services or management for data processing, web hosting, Internet, intranet, telecommunications and information technology.

Data centers in the state were classified based on tiers as defined by the Uptime Institute.<sup>28</sup> As a result of the survey, it was determined that most data centers were either Tier 1 or Tier 2, while four were Tier 3 and one was classified as Tier 4.

The Tiers were defined as follows:

**Tier 1**

- Single non-redundant distribution path serving the IT equipment for mechanical, electrical, and plumbing.
- Non-redundant capacity components.
- Basic site infrastructure with expected availability of 99.671 percent.
- May or may not have raised flooring, UPS, or engine generator.
- Single path for power and cooling distribution, without redundant components.

**Tier 2**

- Meets or exceeds all Tier 1 requirements, plus:
- Redundant site infrastructure capacity components with expected availability of 99.741 percent.
- Has raised flooring, UPS, and engine generator.
- Single path for power and cooling distribution with redundant components.

**Tier 3**

- Meets or exceeds all Tier 1 and Tier 2 requirements, plus:
- Multiple independent distribution paths serving the IT equipment.
- All IT equipment is dual powered and fully compatible with the topology of a site's architecture.
- Concurrently maintainable site infrastructure with expected availability of 99.982 percent.

**Tier 4**

- Meets or exceeds all Tier 1, Tier 2 and Tier 3 requirements.
- All cooling equipment is independently dual powered including chillers and heating, ventilating and air conditioning (HVAC) systems.
- Fault tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995 percent.

<sup>28</sup>Uptime Institute, LLC. (2012).  
"Data Center Site Infrastructure  
Tier Standard: Topology"

Based on the survey responses, the Executive branch of state government operates 28 data centers and 57 server rooms with 37 percent of server rack space is available statewide.

On average, they are between 1000 and 2000 sq. ft. with the one exception of the ADOA data center, which is about 10,000 sq. ft. On average, rack utilization in each of the data centers is 60 percent with eight in the 80-90 percent range. Investments in planned upgrades in all the data centers total about \$28 million over the next 5 years.

A *server room* was defined as a room used to host, power and operate computer servers and their associated components. This room is NOT part of a data center, may be located in a building that is primarily used for business operations, and may share power and/or cooling with the rest of the building.

Sixteen Budget Units have single server rooms while twelve of them have two to five rooms. Most server rooms are approximately 100 – 400 sq. ft. with three server rooms slightly less than 2000 sq. ft.

All server rooms have less than 25 racks each with an average utilization of 60-80 percent. Planned server room facility and equipment upgrade investments total approximately \$5 million.

The expense of operating and maintaining IT facilities is material. In fact, subject matter experts put the total cost of ownership (TCO) for a computer *facility* higher than the TCO of the *IT equipment* housed within it. This is particularly true of computer facilities that are underutilized. It is difficult to justify multiple, underutilized IT facilities that have high costs associated with maintaining and operating core common capabilities such as cooling, humidity control, data cabling, electrical service, fire suppression and security controls.

Many state agencies have chosen to create and operate their own IT facilities with their own equipment and staff resulting in redundant facilities, staffing and equipment.



To better manage and achieve visibility on IT assets statewide, efforts are underway to integrate the data collection process with procurement and the new enterprise resource planning system. It is expected to be a multi-year effort that includes process changes and new reporting capabilities.

### Case Study: Virginia

In 2003, the Virginia Legislature passed HB 1926 and SB 1247 to consolidate the State's technology oversight under a single CIO appointed by the governor. The legislation also created the Virginia Information Technology Agency (VITA) and the Information Technology Investment Board. In 2005, VITA and the Board awarded a \$2.4 billion, 10-year contract to consolidate, update and manage the State's computing infrastructure.

*"The partnership will standardize and modernize the Commonwealth's IT infrastructure capabilities to better serve Commonwealth agencies, higher education institutions, private sector businesses and citizens. The partnership will continue to build upon VITA's current capabilities and will deploy a first-class IT infrastructure for the Commonwealth. The vendor will support VITA in its IT infrastructure transformation of 85 executive branch agencies."*<sup>29</sup>

In December 2008, the Virginia Joint Legislative Audit and Review Commission issued an extensive report detailing performance problems and transition delays. It concluded that the private/public partnership was not likely to produce any of the anticipated cost savings and could potentially increase IT spending.<sup>30</sup>

Owing to significant performance problems and evidence that it would cost more to terminate than continue, the contract was renegotiated in April, 2010.

*"The Virginia Governor announced Tuesday, April 6th, that the state has renegotiated its IT services and management agreement, a \$2.3 billion deal that has been plagued by cost overruns and service problems. The new terms add \$105 million in cash payments to the vendor over the next decade, but state officials said that the expenditure was preferable to killing the deal outright, which would've cost Virginia "at least \$353 million if terminated for cause and \$685 million if terminated for convenience."*<sup>31</sup>

<sup>29</sup>IT Infrastructure Partnership. (n.d.) Retrieved from <http://www.vita.virginia.gov/itpartnership/default.aspx?id=377>

<sup>30</sup>Interim Review of the Virginia Information Technologies Agency. (2008). Retrieved from <http://jlarc.virginia.gov/reports/Rpt381.pdf>

<sup>31</sup>Virginia Restructures IT Services Deal with Northrop Grumman. (2010, April 7) Retrieved from <http://www.govtech.com/policy-management/Virginia-Restructures-IT-Services-Deal-With.html>

<sup>32</sup>Agilisys. (2011, Feb. 15).

“Audit of Northrop Grumman’s Performance Related to the DMX-3 Outage and Associated Infrastructure”. Retrieved from <http://voices.washingtonpost.com/virginiapolitics/Northrop%20Grumman%20Audit.pdf>

<sup>33</sup>Cooney, M. (2006, December 1).

“IBM wins Texas-size data center consolidation contract”. Retrieved from [http://www.computerworld.com/s/article/9005592/IBM\\_wins\\_Texas\\_size\\_data\\_center\\_consolidation\\_contract](http://www.computerworld.com/s/article/9005592/IBM_wins_Texas_size_data_center_consolidation_contract)

<sup>34</sup>Williams, M. (2008, November

7). “Texas puts IBM on notice for data backup deficiencies”. Retrieved from <http://www.govtech.com/budget-finance/Texas-Puts-IBM-on-Notice-for.html>

Virginia’s problems continued in 2010 with a storage system failure that caused an extended loss of service to 26 of 89 state agencies for more than a week. The Virginia Division of Motor Vehicles, one of the most visible of the affected agencies, could not issue or renew drivers’ licenses for more than a week.<sup>32</sup>

### **Case Study: Texas**

Similar to Virginia, in 2005 Texas awarded a seven-year, \$863 million contract to consolidate the state government’s 31 data centers into two facilities in Austin and San Angelo. The project was expected to take two years and save \$159 million over the life of the contract.<sup>33</sup>

In 2008, the Texas Department of Information Resources (DIR) issued a Notice to Cure to the vendor. The notice was issued a week after Governor Perry ordered a temporary stop to the consolidation owing to concerns over failed data backups.<sup>34</sup>

In 2010, DIR issued a second Notice to Cure to the vendor asserting that it had repeatedly underperformed and under-delivered on the contract. At this point, five years into the contract, it was estimated that only 12 percent of the consolidation had been completed.<sup>35</sup>

The situation between Texas DIR and the vendor did not improve and DIR ultimately terminated the contract. In January 2011, more than five years after the award of the original contract, Texas rebid the contract to multiple vendors.<sup>36</sup>

### **Case Study: Oklahoma**

Oklahoma’s six-year IT overhaul project involves unifying technology systems from 135 agencies across Oklahoma into one agency. So far, the Governor said in an interview, IT operating costs have fallen from \$264 million per year in 2009 to \$219 million last year.<sup>37</sup>

<sup>35</sup>Towns, S. (2010, July 16). “Texas warns IBM of outsourcing contract failures”. Retrieved from <http://www.govtech.com/pcio/Texas-Warns-IBM-of-Outsourcing-Contract.html>

<sup>36</sup>Pariseau, B. (2011, January 31). “Texas rebids IBM data center consolidation project”. Retrieved from <http://searchdatacenter.techtarget.com/news/2240031466/Texas-rebids-IBM-data-center-consolidation-project>

<sup>37</sup>Goldber, M. (2013, April) “Oklahoma IT Consolidation Sets Stage for Analytics Use Cases” <http://data-informed.com/oklahoma-it-consolidation-sets-stage-for-analytics-use-cases/>

<sup>38</sup>Wood, C. (2013, April) “New York State and SUNY Partner for Data Center Consolidation” <http://www.govtech.com/e-government/New-York-State-SUNY-Partner-Data-Center-Consolidation.html>

Along with making IT operations more efficient—the State posts an online dashboard to show if IT is meeting service level response targets—the Governor said the strategy enables state policy makers to analyze new dataset combinations. The goal is first to bring together repositories of data “so that we can start formulating a comprehensive data dictionary, or data structure, that will then allow us to provide services where before it was not possible,” he said.

### **Case Study: New York**

As part of a larger effort to rework the State’s IT infrastructure, New York State Gov. Andrew Cuomo announced on April 10, 2013 that the State’s approximately 50 data centers spread across New York would be consolidated, saving the State an expected \$1 billion over the next 20 years, or \$50 million yearly, according to the governor’s office.<sup>38</sup>

The data centers will be housed at the State University of New York (SUNY) College of Nanoscale Science and Engineering (CNSE) and managed in a partnership between CNSE, the New York State Office of Information Technology Services (ITS), and the New York State Office of General Services (OGS).

The data center that will be housed at CNSE is not only intended to serve as a consolidation and optimization effort, but also a means to spur economic growth and promote innovation that benefits the state.

CNSE is not a traditional school, according to Steve Janack, CNSE vice president for marketing and communications, because the college not only has students, but also houses more than 300 private high-tech companies from around the world that are researching, developing and commercializing nanotechnology. Nanotechnology, Janack said, can be applied to many other fields of technology, including ones that interest state and local government, such as energy and biotechnology.

“In one location, you have private industry co-located with the college, so there is a great opportunity to cross-pollinate in terms of the innovation that happens within the information technology industry,” he

said. “By having the data center located here, there are incredible advantages for New York State in terms of consolidation and cost efficiency, and being at the cutting edge of innovation to be able to deliver better services to New Yorkers.”

The move is mutually beneficial, though, Janack said, and should be viewed as a partnership, not just as the college taking over the state’s data center responsibilities. “For the college, it’s an opportunity for faculty and students to be able to integrate with individuals from New York State’s IT workforce,” he said, “and to develop new technologies, new processes, new systems for being able to deliver services efficiently and cost-effectively.”

The data center consolidation is part of the Governor’s larger move toward efficient technology and government. When finished, the state’s entire IT infrastructure consolidation, including the data center move to the new 50,000-square-foot space, is projected to save \$100 million annually. The new data center is planned to be a Tier 3 data center, which indicates a 99.982 percent uptime, compared to a 99.671 percent availability promised by Tier 1 data centers.

### **State Data Center (SDC)**

The State Data Center (SDC) currently houses technology systems mission critical to the continuity of business at the State. Nearly every state entity leverages the SDC’s infrastructure, services, and capabilities. Ensuring these systems are operational and secure is critical to the functions of the State. The management and staff of SDC understand the criticality of our mission, and provide services and support 24/7/365 to ensure that all functions needed by Arizonians across the state are provided with the optimal services available.

In July 2011, the SDC suffered a major outage. The single 18 year old Uninterruptable Power Supply (UPS) blew a fuse on a Friday night. A UPS normally lasts about 15 years and this UPS was three years past typical end of life. One of the major problems with a UPS this old is that it only beeps and flashes lights to notify staff of a problem rather than notify services via text, email or telephone as is possible

with newer equipment. On the Sunday following the UPS' blown fuse, the power to the facility dropped and the UPS wasn't able to respond, putting the building on backup batteries while the diesel generators kicked in. This caused the entire SDC to go temporarily "dark" and many of the systems housed at the SDC did not fully recover when the power was restored. At that time, the blown UPS fuse was discovered and the Power Distribution Units (PDUs) could not come back online without manual intervention. Several Computer Room Air Conditioning (CRAC) units would not restart. The mainframe suffered a serious corruption issue as a result of this incident.

In response, a detailed analysis was done evaluate necessary investments in the SDC. The analysis identified multiple critical upgrades to the supporting infrastructure including enhancements to the physical environment as well as specific hardware and software enhancements. As part of the 2013 - 2015 Transformational Initiatives, the SDC upgraded several critical aspects of the facility, providing redundancy and continuity of critical electrical systems, generator capability, and increased computing capacity to respond to agency customer processing needs. During this period, the State made more than \$5.2 million in SDC related capital investments. These investments included two new Uninterruptible Power Supplies (UPS), a network refresh, electric wiring upgrades, server storage expansion, server and mainframe backup storage expansion and a back-up generator for the Tucson data center.

Of this \$5.2 million was a \$2.9 million SDC Facilities Refresh Project, which included the upgrade of one of the Uninterruptible Power Supplies (UPS) to a higher capacity (750 kVA) and the purchase of an additional UPS of equal capacity, providing a redundant power path to equipment in the SDC. This eliminated a long standing "single point of failure" problem. In addition, this project included the purchase of six new Power Distribution Units (PDU), the update of several PDUs that were at the end of their life cycle, and the purchase of four new Computer Room Air Conditioning (CRAC) Units to improve the cooling capacity in the SDC. The benefit of this was apparent during a recent power outage in the Capitol Mall caused by a lightning strike to an electrical transformer. This incident caused multiple outages at other agencies in the Capitol Mall area, but the SDC continued to operate without an outage.

In the Tucson Data Center (TDC), the new generator provides clean, conditioned power to TDC. Room 2 (“the DR Room”). This enables additional customers including Criminal Justice Commission, DOR, and DES to collocate their Disaster Recovery equipment in this room. This project also included the purchase of 21 new power cables or “whips” to support new upgraded carrier equipment installed in five racks in TDC Room 1 (“the Production Room”).

The SDC implemented a 10 Gigabit Network Infrastructure upgrade to alleviate the performance impact of a bandwidth bottleneck resulting from backups that previously had been running 21 hours out of 24 hours a day.

The SDC also installed an overhead system for distributing power to the third floor servers and other powered devices. This system allowed under-the-floor cabling to be removed increasing the effectiveness of the CRAC Units by opening the airways under the floor that were clogged by this cabling’s obstruction of air flow. This increased the overall effectiveness of the CRAC Units, as well as provided a modern power distribution fully capable of supporting both current and future equipment needs.

Additional Data Backup and Recovery-Storage Capacity licenses were purchased to meet increased current and future requirements of agency customers located at the SDC. Prior to this purchase, the SDC storage back-up system frequently ran at over 99 percent of capacity. Storage back-ups now run in just hours which previously took most of the day to complete.

Tape Storage Devices were added as an additional measure to keep the SDC open systems and mainframe backups from failing due to lack of storage capacity. Four tape drives, two for open systems, and two for the mainframe have also been purchased.

The SDC also upgraded the storage director with 8 Gigabit fiber channel connections to improve functionality and performance.

An SDC inspection after a major outage in August of 2013 revealed that direct power cables should be replaced due to end of life, as well as to meet code compliance. In response, SDC replaced 112 power cables (“whips”). This mitigated the risk of potential fires from substandard whips.

Also in FY 14, the SDC purchased a virtual tape storage subsystem and located it at the Department of Economic Security (DES) DR site which communicates with the virtual tape storage subsystem at the SDC. This rectified the risk represented by the lack of a device to replicate the virtual tape data of the SDC mainframe customers.

Other project expenditures included the purchase of catalog software to manage and report on access to customer data files stored on both disk and tape.

Additionally, as the agency customer demand reached the maximum available mainframe capacity, two additional CPUs, already residing within the current Z/10 mainframe system, have been temporarily activated. This action increased the total processing capacity by 19 percent from 1612 to 1919 Million Instructions per Second (MIPS). This bridged SDC’s mainframe capacity to meet customers’ demand until a new mainframe system could be installed. The contract for these two additional CPUs cost \$450,000 for a ninety day period. A new mainframe is scheduled for implementation in the second quarter of FY 15.

In hindsight, knowing the complexities and risks, ADOA-ASET would probably have opted for moving to an alternative data center sooner. But at the time, that option seemed too large, costly and riskier than fixing the identified issues.

#### **DES Data Center Relocation**

The Department of Economic Security (DES) currently houses their computing infrastructure in an aging data center in Phoenix. During the past 24 months, DES experienced at least four major outages, which required emergency services and evacuation, as well as numerous other minor outages. These incidents

included fires, floods and water leaks, power outages, asbestos abatement, generator problems (including diesel fuel leaks and toxic fumes release) and multiple halon (fire suppression gas) deployments. At this time, the DES data center has deactivated the fire suppression system and removed the halon, leaving the center at risk. There are also concerns of the structural integrity of the facility's raised-floor (floor that is raised 12-18 inches above the foundation to allow for cabling and air-flow for computing equipment).

DES, in partnership with the Governor's office and ADOA-ASET, weighed the alternatives of repairing the current facility or contracting with an outside facility to host the computing equipment. The physical and monetary assets required to repair the facility and completely abate risks are significant. An initial repair investment would only temporarily relieve these risks. The ongoing capital expenditures to continuously maintain the facility would further burden an already stressed budget.

Working with subject matter experts from Gartner, it was determined that an outside facility to house the computing equipment currently located within the DES data center would allow DES to redirect resources to focus on delivering quality services to the State and away from patching aging infrastructure.

This resulted in the September 2014 decision, to award a statewide contract for an alternative data center and transition the DES systems over the next two years as mentioned in Overview section.



# Cloud Computing



## Overview

- A. By 2017, public cloud offerings will grow to account for more than 25 percent of government business services in domains other than national defense and security.
- B. The IT industry faces an acute shortage of skills (additional information may be found under the “IT Personnel” section). Organizations will be forced to evolve from installing servers to managing integrations, provisioning services, and negotiating vendor relationships. Cloud computing enables organizations to become increasingly agile and responsive to changing business conditions.
- C. Due to federal disallowed expenditures (refer to a later section in this study), pay-as-you-go or pay-for-what-you-use (metered) models offered by cloud computing represent attractive options to the State.
- D. Regulatory compliance prevents costly fines. The multibillion-dollar cloud computing business relies in part on cloud vendors’ ability to secure customers’ data. Cloud providers adhere to standards designed to provide high levels of security. The State benefits because security actually increases when using cloud solutions due to strict security standards to which cloud providers must adhere. In addition to the regular security audits, providers meet FedRAMP, NIST, FISMA, PCI DSS, HIPAA, and other requirements.
- E. Cloud service providers host their data centers in hyper-secure facilities where access controls are multi-layered and tightly controlled. The average state BU may be challenged to achieve this level of security using an on-site solution. Each BU balances other focuses and considerations when allocating staff access, usability, space, budget, skills and resources. Cloud computing provides layered security,

an approach that includes critical elements like encryption, key management, strong access controls, and security intelligence thereby improving data security.

- F. Cloud computing forces software applications to run the latest versions, making security patches and program updates easier to keep current. BU IT staff may not be adequately trained in cybersecurity, so these automatic updates help maintain overall business security.
- G. Cloud computing offers a less expensive option for state BUs because vendors enjoy massive discounts from hardware manufacturers due to their purchase volume. In addition, BUs are no longer required to focus on facilities-related items like power conditioning, backup power, fire suppression, air conditioning and physical security.

### **Strategy – Promote Cloud Computing as a Viable Alternative to Ownership**

The use of public cloud computing is expanding rapidly and most organizations already exploit public cloud-based resources to run both critical and non-critical business systems. Cloud computing has proven itself and represents a viable alternative to direct investment and ownership of IT infrastructure and services.

Most organizations are now executing strategies that include an increasing volume of application and data migration to the public cloud. This is reflected by the number of funded projects, applications, and data that exist on public clouds in production environments and the usage of public cloud capacity (i.e., instances).

The federal government published a cloud computing strategy, a Cloud First Policy, and established GSA contracts for cloud services. A number of U.S. states have developed cloud strategies for their agencies and many state and local governments currently leverage cloud services.

State agencies should continue to leverage cloud computing and move applications and on-site servers to the cloud where appropriate. This strategy features many benefits including:

- A. Cloud computing reduces the cost of IT ownership by consolidating agency server footprints through cloud and virtualization efforts. Similarly, data center consolidation reduces hardware costs and drastically reduces energy consumption.
- B. Agency programs become increasingly agile and responsive to changing business conditions using the cloud. Cloud adoption models allow the flexibility to deploy more current services with elastic capacity, cloud deployments take less time to provision and are more efficient at building, deploying, testing, and releasing new features.
- C. State agencies benefit from the certifications that cloud computing solution providers have achieved. Many third-party data centers are SOC 1 (SSAE 16 Type II) and SOC 2-audited, ISO 27001 certified and have achieved the U.S. Federal Government's FISMA certification. Agencies do not have the resources to achieve these security certifications and benefit by using cloud computing.
- D. Traditional on-site systems security requires continuous monitoring. Upgrades and patches need to be applied and thoroughly tested. Not all agencies support appropriate resources and skills. Cloud computing vendors install and test patches and upgrades centrally, using more specialist resources. End user applications are automatically updated and patched without the need to involve state IT staff.

### **Detailed Analysis**

Cloud computing is a fairly new, disruptive technology forcing a fundamental shift in how computing resources are accessed and consumed worldwide. In 2011 the U.S. Chief Information Officer issued the Federal Cloud Computing Strategy that requires federal agencies to evaluate safe, secure cloud computing

options before making new investments in technology (Cloud First Policy). The executive summary of this strategy states:

*“The Federal Government’s current Information Technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. These inefficiencies negatively impact the Federal Government’s ability to serve the American public.”*

The Executive Summary also identifies cloud computing as a mechanism to address the identified inefficiencies and improve government service delivery. The Federal Strategy established \$20 billion or approximately 25 percent of federal IT spending as a potential target for migrating to cloud computing solutions.

The United States is not alone in developing a national strategy for cloud computing. The UK, Australia, New Zealand, Canada, Japan, Russia, France, South Korea, and others have similar strategies. A number of them have also built private government clouds for use by their agencies.

A significant number of advertised advantages are associated with the move to cloud computing. The two expectations that appeared most often in our research are the desire to reduce IT capital expenditure and the desire to reduce IT recurring costs.

The key services being moved to the cloud by the surveyed organizations include messaging, conferencing and collaboration, storage, office productivity suites, and business process applications. In this report, more than half of the respondents cited increased efficiency as a benefit of using cloud technology.

### **Cost Analysis**

- A shared email service with 50GB storage per user, per month on premise currently costs \$152.00 vs. \$4.00 for a hosted email exchange that Microsoft offers online as part of Office 365. Estimated savings: \$1,776 per user, per year.
- Domain Name Servers (DNS), the Internet's equivalent of a phone book, maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. The State currently hosts 351 zones and 5,600 records on a global network of DNS servers at a series of worldwide locations through Route 53, a highly available and reliable service from Amazon. ADOA-ASET previously spent \$87,000 per year to host and manage DNS service before migrating the service to the cloud. Route 53 costs ADOA just \$18,000 per year, a savings of \$69,000.
- ADOA-ASET expended \$26,000 per year to provide document management service to its customers before moving the service to a hosted offering that now only costs \$6,000 per year.
- A single virtual server instance with one CPU, 4GB RAM and 100GB storage at SDC costs \$300 per month (not including any support services to repair or keep the server patched) compared to \$111 per month on the cloud. Moving 100 servers from on-premises to the cloud saves the State \$226,000 per year.

### **Office Productivity and e-Mail Platforms**

The IT Inventory data indicates that office productivity software typically used for internal agency administration and communication varies throughout the State. State agencies currently operate twelve different versions of office productivity software from three different publishers. Several of these product versions were released prior to the year 2000. For interoperability, documents created in newer software must be saved in the older formats, thus diminishing the value of the new software. At least thirty-three agencies operate independent e-mail systems in the State using three different products:

Microsoft Exchange, Novell Group Wise, and Lotus Notes. While the IT inventory data for server software is incomplete, it does show seven different versions of these three e-mail systems.

Many state agencies are evaluating moving the burden and risk of e-mail and office productivity to a shared services or cloud-based model. Benefits include standardizing communications, improving collaboration, reducing risk, reducing costs, and ensuring license compliance. Some agencies including ADOA, have already completed this move.

New York and Texas began their IT modernizations by consolidating e-mail and productivity software licensing and administration to a centralized state agency then, subsequently, decided to further optimize by moving to a cloud-based solution. In both cases they are migrating more than 100,000 users, including their healthcare users. New York expects to complete the migration within five months.

The Arizona Department of Veteran Affairs, Auditor General's Office and Department of Administration converted their email service to Office 365; a managed, cloud-based offering from Microsoft. Other state agencies are in the process of adapting Office 365 as their email solution.

# Arizona Network (AZNet II)



As of 2011, Oklahoma lacked a centralized telecommunications and network infrastructure. Networking equipment consisted of a mixed set of vendors and vendor models. The lifecycle of deployed equipment was in various stages of support and some was at end of life. The State did not utilize a consistent set of tools for monitoring the network. No statewide sets of metrics existed to measure and compare network performance. Oklahoma's current initiative includes replacing obsolete networks with a standardized, unified system featuring leading technology.

In comparison, Arizona has maintained a centralized network and telephony program for years and leverages carrier services for supporting the majority of the infrastructure. AZNet, a consolidated telecommunications program, provides State of Arizona agencies, boards and commissions with outsourced voice and networking services and equipment contracted at a predictable, user-based monthly charge. AZNet II represents the second major phase of the program. A refresh of the entire network is underway, including the implementation of a statewide Voice over IP telephony system.

## Overview

- A. AZNet II provides voice and data capabilities for more than 33,000 state employees from 124 agencies.
- B. There are over 19,000 carrier circuits connecting 741 facilities across the entire State.
- C. AZNet II handles more than 500,000 calls and three terabytes of data transactions on a daily basis.

## Strategy – Provide Core Telecom and Network Infrastructure; Refresh the Entire Network

AZNet II serves as the voice, video and data communications backbone for almost all state agencies. The large-scale data network is vital to the continuity of government, ensuring the secure transmission of information between the 741 state facilities.

Optimizing and refreshing the entire network represents an ambitious goal the State has been executing on over the past two years. One of the key goals of the second-generation AZNet (or AZNet II) contract includes refreshing the entire state network and moving to Voice over Internet Protocol (VOIP). The contract accomplishes this by moving the responsibility of the contractor into state buildings and managing the internal networks. To date, this approach has been a very successful part of the program, benefiting many agencies statewide. Almost two years remain on this part of the program.

Telecom Expense Management represents another major component of the new contract. Separating the billing and reconciliation process from the primary vendor allows for clear and transparent processes to ensure that the State is billed appropriately for services used.

Increased transparency is a third major priority. New implemented initiatives ensure that competitive processes are followed for carrier, cabling and other telecom / network related services.

#### **Detailed Analysis**

AZNet II provides state agencies, boards and commissions with a cost effective, efficient and consolidated shared telecommunications and network infrastructure. AZNet II supports voice, data and internet services for government agencies, their employees and the public. Although not a large-scale computing system as defined by the study, AZNet was included due to the service magnitude and value to the State.

Arizona Revised Statutes § 41-712 (Laws 2005, Chapter 301) directed ADOA to establish a Telecommunications Program Office (TPO) for the oversight of a single statewide telecommunications network called AZNet. State agencies enter into a contract through the TPO for their telecommunication needs, including the installation and the maintenance of telecommunications systems. The TPO ensures that its contractor acts as the State's agent for all carrier services to the offices, departments and agencies served by AZNet.





**33,000  
Employees**



**124  
Agencies**



**19,000  
Circuits**



**741 Locations  
(133,000 sq. miles)**



**500,000 calls  
3TB of Data**

AZNet manages voice and data connectivity for more than 33,000 state employees from 124 agencies statewide. ADOA contracted with a vendor responsible for managing over 19,000 circuits to 741 state locations encompassing over 113,000 square miles. The AZNet network processes an average of over 500,000 phone calls and three terabytes of data transactions on a daily basis.

AZNet provides enterprise equipment connecting voice, data and security to data centers supporting geographically redundant connections and enabling fail over protection throughout the State.

As part of the statewide outsourcing contract, all existing core voice, network and security components were replaced with new equipment at designated state data centers. All agency switches, routers and desktop phones are currently being replaced with new equipment as an additional requirement of the outsourcing contract.

The State of Arizona benefits from the outsourcing contract moving from a federated to a consolidated voice and network service model. Consolidation reduces the continuous need for numerous maintenance contracts, moving to a more cost effective enterprise model.

The AZNet statewide voice and network contract requires the vendor to refresh all core voice, network and security systems as well as 741 state locations with new routers, switches and telephone sets. The seat pricing includes new equipment and service capabilities provided within the scope of the statewide contract, thus eliminating the need for upfront capital investments for voice and network services. This approach allows for a more budget friendly, predictable cost structure for agencies, boards and commissions.

The voice and network infrastructure is 100 percent completed with core systems in four state data centers providing redundant fail over protection. The agency voice and network refresh project is approximately 30 percent complete with nearly 22,000 network seats and 16,000 voice seats upgraded.

The benefit of this refreshment project includes replacement of existing end of life and end of support equipment. The existing equipment vendors no longer support maintenance on all core and agency equipment. State agencies realize additional benefits of having increased voice and network capabilities that the old systems were unable to provide. Monthly seat contract pricing includes all equipment, requiring no capital investment.

The Telecommunications Expense Management (TEM) contract provides a single point for all telecommunication billing to be processed. The TEM vendor provides an independent arbitrator of billing disputes between the AZNet and carrier service providers and the agencies. In the previous contract, the AZNet provider also acted as the TEM provider. It was extremely difficult to resolve billing disputes when the provider was also the arbitrator of their own services.

The ASET-EIC (Enterprise Infrastructure and Communications) group implemented stringent yet transparent processes and procedures for Carrier Service Circuit awards. Agencies depend on carrier service circuits to provide voice, data and internet connectivity to office locations throughout the State. All carrier service circuit awards are based upon Total Cost of Ownership (TCO) for the agencies, providing the best possible service at the most cost effective rates. ASET-EIC achieves transparency by posting all carrier services circuit awards to the website on a monthly basis.

The ASET-EIC group also implemented similar processes and procedures for the statewide cabling contract. State agencies often require cabling for telecommunications needs. The Cabling and Power Manager in ASET-EIC works with Agencies to set up vendor site visits and develops a scope of work. All vendors on the cabling contract are contacted and requested to participate. ASET-EIC receives vendor pricing based upon the scope of the work outlined at the site visits and shares it with the agencies, enabling them to receive the best possible service at the most cost effective rates.

# Enterprise Capabilities



## Overview

- A. Citizens, businesses and employees require services to be available anytime, anywhere and from any device. To improve the quality and capacity of business services and foster collaboration and data sharing requires flexible foundational technologies and core enterprise capabilities.
- B. The State has implemented multiple statewide enterprise capabilities. Application examples include finance management / accounting, human resources, payroll, procurement, inventory / asset management, facilities management. Infrastructure examples include network, telecommunications security, data center, mainframe, servers and cloud.
- C. The Arizona Enterprise Services Platform (AESP) is a secure cloud based platform that provides web / application hosting, online payment processing, an Application Programming Interface (API) store, and an identity and access management system.
- D. AESP supports 95 state agencies with over 150 websites and applications, 30 of which collect payments and generate revenue for the State.
- E. AESP secure payment engine (i.e. credit card payment system) processes than 420,000 transactions representing over \$70 million in revenue every year. The secure payment engine is integrated into the State accounting system and provides end-to-end commerce capabilities.
- F. The platform includes web-hosting capabilities for agency websites based on a responsive (phone, tablet or computer ready) design that is accessible for persons with disabilities and has rich built in analytic and administrative capabilities. More than 70 new agency websites have already deployed on this platform. The agency platform showcase profiles these new sites: <https://showcase.az.gov/gallery>.

- G. To increase the quality of applications and accelerate innovation, the platform now supports an Application Programming Interface (API) store. In simple terms, an API is a method for allowing one application to securely pass data to another application. There are six APIs currently available: Arizona Winning Lottery Numbers, Arizona City / County Directory, Arizona Corporation Directory, State Agency Directory, State Agency Services and State Employees.
- H. With the launch of the new state accounting system in July of 2015, a statewide single sign-on capability will be incorporated on the platform. This single sign-on feature will be available to all state agencies to incorporate into their applications, allowing for better management of user access to state systems.

### **Strategy – Expand Adoption of Secure Statewide Enterprise Capabilities**

Arizona has taken advantage of many statewide enterprise capabilities such as finance management, human resources, payroll and procurement. The State has also consolidated mainframes, implemented a statewide network, and invested in core data center and cloud capabilities.

Enable citizens, businesses and employees to access state services anywhere and at any time. State websites and applications should continue to be designed to operate on any device and support accessibility natively. By providing secure websites that aggregate content, provide users with personalized experiences and allow users to utilize online services, the State will be able to drive efficiencies and improve customer satisfaction.

Provide secure, reusable, containers to increase the velocity of service delivery. The Arizona Enterprise Services Platform (AESP) is an extensible system that allows agencies to develop websites and applications without having to build solutions from scratch. The capabilities include identity management (e.g. single sign-on, multi-factor authentication, etc.), analytics, payment processing, integration to the State financial system, and a business rules engine, among others. Future capabilities may include forms management, workflow management, document management, digital signature and subscription / notification capabilities.

Leverage Application Programming Interfaces (APIs) to foster collaboration and increase quality. The State has enormous amounts of data, much of which is in agency silos or application silos. The State should continue to implement APIs and develop secure methods to share this information between agencies and interested third parties. Data sharing can help improve the quality of services of agencies and can also potentially be used as new revenue models to offset costs.

Agencies should employ strong application portfolio assessments and rationalizations. Legacy applications and websites can increase security and continuity risks, impact customer and employee satisfaction and have high total cost of ownership. The State should systematically assess essential application capabilities. The State should continue to develop business analytics capabilities. The State is currently in the process of deploying tools for business analytics as part of the Enterprise Resource Planning (ERP) project that can potentially be used to gain valuable insights and enhance the government services effectiveness. Some potential uses of business analytics by state and local government agencies include: cyber security, public safety, fraud detection – tax collection, education and transportation.

### **Detailed Analysis**

IT systems and capabilities exist only to serve business needs. These capabilities can be used to automate and scale business capacity. They can also be used to transform how organization operate and deliver services to their customers. Some capabilities are used in specific functional areas such as accounting while others are used across an entire organization like time sheets. Capabilities can be unique and used to differentiate the organization while others can be generic across many organizations. They can be operated internally, outsourced completely or take hybrid approaches.

### **Arizona Portals**

There are many opportunities to improve how state government communicates with its stakeholders. Citizens, businesses and government employees have some very similar and extremely different needs. AZ.gov is the online, public gateway for all of Arizona. The site has been redesigned to provide essential information for people interested in learning more about Arizona's past and future; business and

employment opportunities; education and residential information; activities for resident and visitors and government.

Sometimes users need more than public access. Users today want personalized experiences that allow them to interact and to complete services online. Many states like Michigan (<http://www.michigan.gov/business>), Virginia (<http://businessonestop.virginia.gov>) and South Carolina (<https://www.scbos.sc.gov>) have developed portals that cater to doing business within the State. These portals are sometimes called “business one-stop” solutions. These “business one-stop” portals provide businesses with key information about starting, running or expanding businesses within their state. The sites also provide compelling reasons why to open or expand in their state versus another. These sites have links to important regulations, processes, licensing information and resources. Per A.R.S 41-3504, Arizona is currently in the process of implementing a similar “business one-stop” solution.

Citizens and employees also need access to secure, personalized services. Arizona is creating a new service, called my.az.gov, that will help all Arizonans find the information and services they need across Arizona Government. Rather than organizing services around the agencies that deliver them, my.az.gov will organize services around the needs of Arizona citizens, businesses and employees, helping them to get the information they need, when they need it.

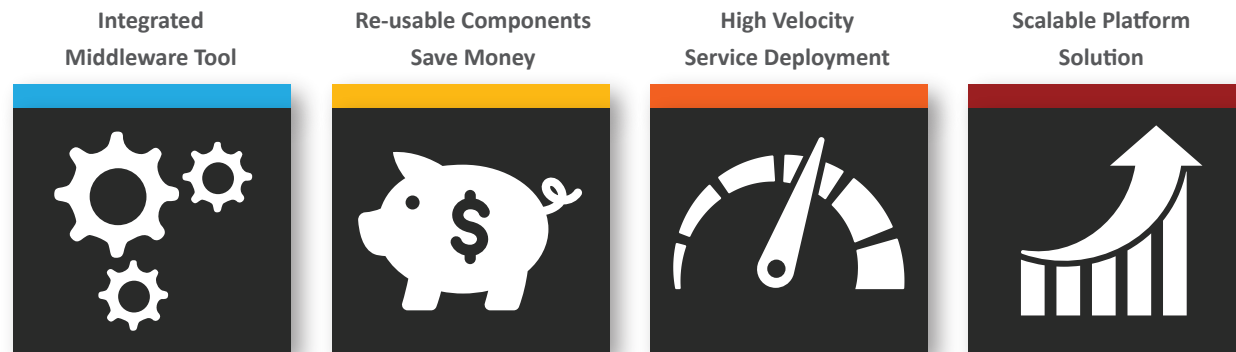
In particular, citizens and businesses have a fundamental problem navigating Arizona Government’s myriad of resources across hundreds of different websites. It can be difficult to locate information about services available in a particular neighborhood, to find the correct forms to start a business, or to get the status of a license application. The team at my.az.gov is working to solve these problems. The project team will build and beta-test new features and tools with the purpose of modernizing the way Arizona Government interacts with its constituents.

my.az.gov will save people and businesses time when transacting with the government, increase awareness of available government services, and speed up notifications and updates. my.az.gov has the

potential not only to save Arizonan’s time and money, but to dramatically change how they communicate with and view their government.

**Platform and Application as a Service**

In alignment of the cloud strategy, the State needs secure, reusable, platform and application containers to increase the velocity of service delivery. The Arizona Enterprise Services Platform (AESP) is an extensible system that allows agencies to develop websites and applications without having to build solutions from scratch.



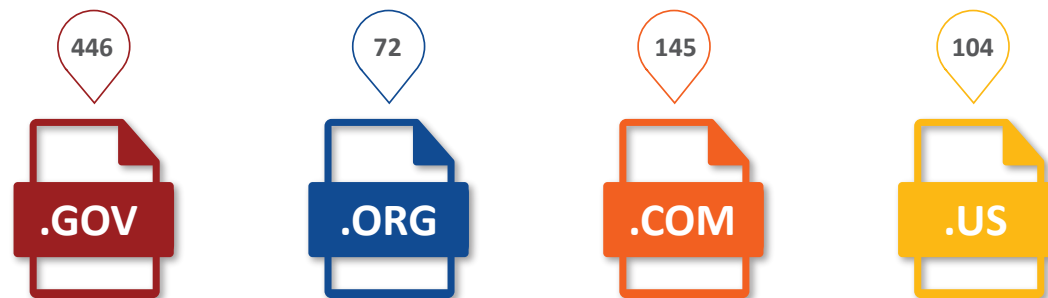
Reusable and scalable platform containers that provide pre-configured solutions with operating systems, databases and middle ware components allows agencies to save time and money for valuable system engineering resources. These key resources can spend time working on integrations that drive value for the business and the end users.

Application containers include many capabilities such as identity management (e.g. single sign-on, multi-factor authentication, etc.), web and application analytics, payment processing, integration to the State financial system, and a business rules engine. Future capabilities may include forms management, workflow management, document management, digital signature and subscription / notification capabilities.

The platform currently supports more than 150 online applications of which over 30 process online payments today. State agencies have more demands for additional online services than the State can currently support. Benefits of online automation, a convenience to our citizens and businesses include: allowing real-time form validation and ensuring 100 percent completion of forms; increasing the quality of the application by enforcing business rules at the time the form is being filled out by the end user; enabling online credit card processes; integrating directly with the State accounting system and the State bank reducing workload and errors; and improving security by leveraging the core security capabilities of the platform.

**Public Documents on the Internet**

The LSCS study also directed ADOA-ASET to conduct a study of “The number of public documents that are available on the Internet and the potential costs savings that could be obtained by making more documents available on the Internet. Any recommendations that result from this study shall require that state documents and information use non-proprietary industry sitemap protocols and search engine mapping.”

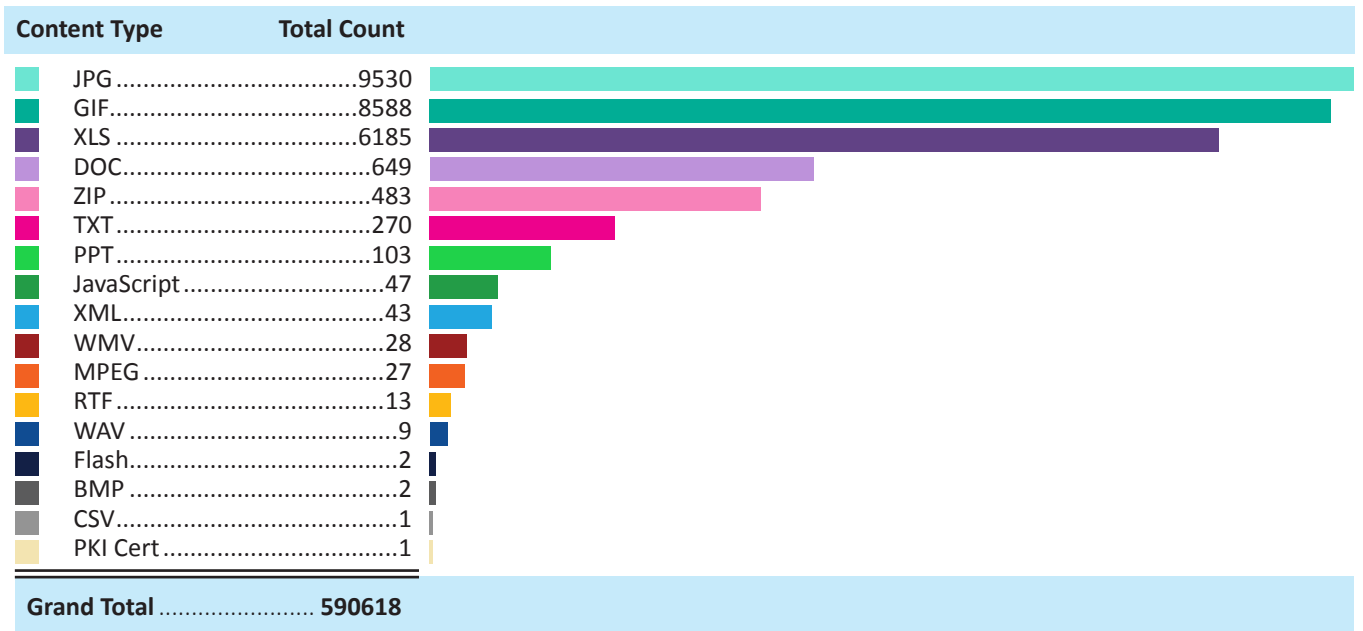


The State currently has 1,154 public facing Uniform Resource Locators (URLs) or website addresses. Of these 343 are system specific and do not have friendly user interfaces and 47 are specific to online email sites. The remaining 764 URLs are a combination of agency websites (or sub-sites) or applications of which 446 are registered as “.gov domains”, 72 as “.org domains”, 145 as “.com domains, and 104 “.us domains”.





Content Type	Total Count	Content Type	Total Count	Content Type	Total Count
<b>JavaScript</b>	<b>47</b>	<b>MPEG</b>	<b>27</b>	<b>Flash</b>	<b>2</b>
DHS.....	47	AHCCCS.....	1	AHCCCS.....	1
XML.....	43	DEQ.....	13	DEQ.....	1
AHCCCS.....	23	DHS.....	13		
DOR.....	16			<b>BMP</b>	<b>2</b>
DOT.....	1	<b>RTF</b>	<b>13</b>	DOR.....	2
DOA.....	3	AHCCCS.....	4		
		DEQ.....	1	<b>CSV</b>	<b>1</b>
<b>WMV</b>	<b>28</b>	DHS.....	7	DOT.....	1
AHCCCS.....	6	DOT.....	1		
DEQ.....	4			<b>PKI</b>	<b>Cert 1</b>
DHS.....	9	<b>WAV</b>	<b>9</b>	DEQ.....	1
DOC.....	4	DHS.....	9		
DOT.....	5				



PDF, Excel and Word documents seem to be most prominent file types agencies use to publish documents online. A challenge with some of the document types is that the data residing in them cannot be searched, indexed or analyzed. While a number of agencies are investing in web applications to capture, store, index, and analyze the data the process of doing so is inconsistent. The state could benefit significantly from standardizing this process through data governance and master data management (MDM).

### **Application Programming Interfaces (APIs)**

Brian Koles wrote an article titled A Company Without APIs Is Like a Computer Without Internet - in which he states, "Application Programming Interfaces are the conduits through which data, platforms and goals come together".<sup>39</sup>

Jeff Bezos, Amazon's founder, mandated that all data and functionality will be exposed via APIs. It is through these APIs that Amazon has become the global marketplace that now sells anything from anybody, not just books anymore.

The Federal Digital Government Strategy<sup>40</sup>, implemented the objective: Make Existing High-Value Data and Content Available through Web APIs. The plan required agencies to: Identify at least two major customer-facing systems that contain high-value data and content; Expose this information through web APIs to the appropriate audiences; Apply metadata tags in compliance with the new federal guidelines; and Publish a plan to transition additional systems as practical. These data sets are made public via Data.gov.<sup>41</sup>

The State has recently started on this journey and has implemented an API Store (<https://apistore.az.gov> – registered access is required). The API Store allows for API creation / registration, security management, usage statistics, usage controls, monetization strategies and many other features. The following six APIs have been implemented and are available:

<sup>39</sup><http://readwrite.com/2013/11/29/company-without-api-computer-without-internet#awesm=~oIGAzBQR7CmmSF>

<sup>40</sup><http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>

<sup>41</sup><https://www.data.gov>

- Arizona Winning Lottery Numbers
- Arizona City / County Directory
- Arizona Corporation Directory
- State Agency Directory
- State Agency Services
- State Employees

The State has a goal to have thirty APIs available by July 1, 2016.

There is still policy and contractual work to be done to ensure appropriate use of data, service level objectives and to simplify agencies' ability to share the information. Training and governance must also be included in this process.

### **Application Portfolio Management / Rationalization**

The business operations and IT budgets of most state agencies are still managed in silos. As a result, agencies are procuring and maintaining multiple systems with similar functionalities on diverse technology platforms. Over time, as the IT landscape evolves with the addition of new business processes, deployment of best fit IT solutions or incremental enhancement to overcome the legacy limitations, the result is a highly integrated, non-standardized, complex and inflexible IT environment. This environment cannot be aligned to the agency's dynamic needs.

While IT teams are working hard to deliver business results with their legacy platforms, agency demands change at a very fast rate. Technology advancement has added further challenges to the mix as newer IT solution areas like cloud, big data, analytics, mobility and social media are driving agencies to transform themselves in order to efficiently deliver services to its customers. The need for an informed portfolio simplification and standardization is imminent in such cases even to realize the envisaged business value from their strategic initiatives.

Application portfolio rationalization is accomplished through shuffling and revamping of the existing application service portfolio, which can include retirement of non-valued applications, elimination of functional redundancy, re-platforming or migration of applications to more standardized contemporary computing platforms and replacement of legacy systems.

A simplified, standardized and optimized application portfolio can deliver the desired level of agility and robustness to an organization, creating the following benefits:

- Fund more innovation by shifting RTB (Run the Business) spend from unneeded applications to TTB (Transform the Business)
- Reducing TCO (Total Cost of Ownership) by retiring applications aimed at meeting the best-in-class benchmarks and eliminating redundancies
- Standardized and simplified business processes, including reducing process variations across agencies
- Reduced number of technologies and technology platforms, including reducing variations and provide opportunity for cost savings due to economies of scale
- Reduced complexity and risk due to aging, siloed or unmanageable systems
- Increased alignment between business & IT, performance and agility by increasing key performance indicators across business processes
- Free-up development resources so they can focus and deliver projects faster

State agencies should employ strong application portfolio assessments and rationalizations. Legacy applications and websites can increase security and continuity risks, impact customer and employee

satisfaction and have high total cost of ownership. The State should systematically assess essential application capabilities.

### **Business Analytics**

State and local government agencies maintain tremendous amounts of data in a variety of diverse systems and databases. Hidden in the immense volumes, variety and velocity of data that is produced today is new information, facts, relationships, indicators and pointers, which either could not be practically discovered in the past, or simply did not exist before. This new information - about citizens, projects, initiatives, operations, and more – effectively captured, managed, and analyzed, has the power to enhance profoundly the effectiveness of government, such as improving public service while consuming fewer resources.

Harnessing data will also serve the key objectives and recommendations described in the Digital Government Strategy report the White House released on 23 May 2012 – “Digital Government: Build a 21st Century Platform to Better Serve The American People” (Digital Government Strategy). A primary component of the Digital Government Strategy is to “unlock the power of government data to spur innovation across our nation and improve the quality of services for the American people”. Business Analytics is a key to fulfill the very essence of this objective.

The State is currently in the process of deploying tools for business analytics as part of the Enterprise Resource Planning (ERP) project that can potentially be used to gain valuable insights and enhance the government services effectiveness. Some potential uses of business analytics by state and local government agencies include:

### **Cyber Security**

State agencies face numerous challenges associated with protecting themselves against cyber attacks, such as managing the exponential growth in network-produced data, database performance issues due to lack of ability to scale to capture this data, and the complexity in developing and applying analytics for

fraud to cyber data. Cyber intelligence and other machine generated data are growing beyond the limits of traditional database and appliance vendors. Therefore, requirements exist for fast data ingestion, data sharing, and collaboration. The State can benefit by delivering innovative cyber analytics and data intensive computing solutions.

### **Public Safety**

Many law enforcement agencies have effectively deployed business analytics to reduce crime rates. By more accurately predicting when and where crimes are likely to occur, and identifying those factors that contribute to illegal activity, these agencies can improve the allocation and deployment of resources, minimize costs, and empower everyone from analysts to officers to more proactively detect and deter crime.

### **Fraud Detection – Tax Collection**

By increasing the ability to quickly spot anomalies, collection agencies can lower the “tax gap” – the difference between what taxpayers owe and what they pay voluntarily – and profoundly change the culture of those that would consider attempting improper tax filings. Most agencies practice a “pay and chase” model, in which they accept returns and often pay out tax refunds, and only ex post facto review a sampling of returns in order to reveal unintentional or intentional underpayment. Business Analytics offers the ability to improve fraud detection and uncover noncompliance at the time tax returns are initially filed, reducing the issuance of questionable refunds.

### **Education**

Through in-depth tracking and analysis of on-line student learning activities – with fine grained analysis down to the level of mouse clicks – researchers can ascertain how students learn and the approaches that can be used to improve learning. This analysis can be done across thousands of students rather than through small isolated studies. Courses and teaching approaches, online and traditional, can be modified to reflect the information gleaned from the large scale analysis.

### **Transportation**

Through improved information and autonomous features, business analytics has the potential to transform transportation in many ways. The nemesis of many American drivers, traffic jams waste energy, and cost individuals time and money. Distributed sensors on handheld devices, on vehicles, and on roads can provide real-time traffic information that is analyzed and shared. This information, coupled with more autonomous features in cars can allow drivers to operate more safely and with less disruption to traffic flow. This new type of traffic ecosystem, with increasingly connected “intelligent cars,” has the potential to transform how we use our roadways.



# IT Personnel



Oklahoma has consolidated its IT staffing and plans to reduce IT FTEs by 29 percent by consolidating data centers and standardizing infrastructure and applications. They anticipate a \$37 million cost avoidance, although it is unclear in their plan if contractor or third-party vendor costs will increase. Gartner reports the average percent of IT employees to non-IT employees is 3.8 percent. Oklahoma's strategy is to reduce their headcount total to 3.6 percent, which is slightly below average.

Arizona's IT structure is still a federated model with only some shared services being leveraged. Strategies for centralization and specialization are currently being implemented through strategic shared services. Arizona has seen some agencies reap rewards for investing in IT. A few specific agencies have as much as 12-16 percent of their staff as IT personnel. IT jobs and skills are rapidly changing as technology is advancing. For example the State needs fewer System Administrators and more Automation Engineers. An overall reduction in IT head count is a short-sighted strategy that will set Arizona back for many years. Many other transformational initiatives will have greater positive impact than reduction in staff (i.e. Security, Networking, Cloud, Enterprise Capabilities, etc.).

As of 2011, Oklahoma's average IT salary was \$78K per employee, which is approximately \$14K higher than Arizona's current average salary. AZ's below market salaries remain a significant challenge for recruiting and retaining talent. Utilizing the lower average salary rate, AZ has potentially realized \$20.6 million annually or \$61.8 million over the past 3 years in cost avoidance. But there are additional costs for turnover, recruiting and lost productivity that should not be underestimated. ADOA-ASET alone had an average of 34 open positions for all of FY14. This was a huge impact on service and project execution (millions in service impact and lost opportunities). The average time to hire IT employees is greater than 85 days and it needs to be considered as a risk and a cost.

**Overview**

- A. The State has more than 1,460 full-time IT employees (4 percent of the total – Gartner indicates industry average of 3.8 percent) and more than 400 contractors.
- B. 27 percent of IT employees at the State will qualify for retirement over the next five years.
- C. Over the past two years, the State has facilitated 13 formal IT training classes with 412 attendees for a total of 8,088 people-hours of training at a total cost of \$199,653 or \$775 per person.
- D. In July of 2014, the State created 13 disciplines and 75 new IT job classifications which provide detailed career paths for employees.
- E. High-level estimate of the costs for IT full-time employees: average salary of an IT employee in the State is \$63,911. Employee Related Expenses (ERE) (per the General Accounting Office) is calculated at 35 percent which is \$22,368.85; estimated overhead at 11 percent is \$7030.21 and operating costs add another 10 percent at \$6391.10 bringing the total to \$99,701 per employee. With 1,474 IT employees listed in the state the estimated annual salary related IT costs are \$146,959,510.

**Strategy – Develop Dynamic Programs to Recruit and Retain IT Talent**

The State’s strategy of developing dynamic programs to recruit and retain it talent consists of the following initiatives:

- Develop robust IT recruitment program to maintain a pipeline of qualified talent. ADOA-Human Resources (HR) recently hired a full-time IT recruiter. Partnering with multiple agencies, ADOA-HR attended multiple job fairs and held an IT open house.
- Continue to invest in high-quality IT training to ensure the State can keep up with skill requirements.

In addition to formal training, continue developing Centers of Excellence (COEs) or working groups to gather IT employees in order to collaborate on common goals.

- Leverage strong governance practices to develop relationships, drive initiatives and develop common policies and tools.
- Partner with the State Procurement Office to develop strategic statewide contracts that provide key resources and services to enable state agencies.
- Invest in talent development through apprenticeship to create a pipeline of loyal skilled workers, increase productivity, and improve the bottom line.

### **Detailed Analysis**

The State of Arizona, including the Legislative and Judicial branches, has more than 170 government entities including agencies, board, commissions, councils, divisions and offices. Across these 170+ entities, there are approximately 1,460 full-time IT employees and roughly 430 contractors supporting IT functions across the State. With approximately 36,100 full-time state employees, full-time IT resources account for approximately 4 percent of the overall total full-time staff.

With Arizona having a decentralized IT model, each agency has the option to maintain its own IT systems and resources. If the agency is large enough to justify having a Chief Information Officer, that individual is responsible for the major IT strategies and functions for that agency. However, there are many state entities that have only a single, full-time IT employee supporting their systems. Regardless of the size of the agency, their most senior technology resource does not report directly to the State CIO, but instead reports to some other Executive-level resource within their respective agency.

Due to this organizational structure, the State CIO relies heavily on a governance model that focuses on relationships and partnerships with agency IT leadership. Although the State CIO has additional “controls” to ensure agency IT projects are adhering to statewide policies and standards, the most

successful approach has been for the State CIO to be the champion of transparency and communication. The result has been an increased level of trust between ADOA-ASET and other agencies and ultimately has resulted in an increase in centralized shared services over the past few years.

From a leadership standpoint, the State has a CIO Council that consists of IT leadership across all agencies and is led by the State CIO. The CIO Council is a working technical advisory committee organized to provide advice and support for statewide information technology issues. It also serves as a forum for reviewing information technology subjects that have common or universal interest for the several executive branch agencies. The Council advises the ADOA-ASET office on technical standards as well as reporting progress on specific projects. ADOA-ASET in turn, uses the meeting for collaborating across the State, communicating status on its projects and issues of concern. Council Task Teams may be periodically organized to explore technical subjects and come up with recommendations for the State CIO.

### **Employee Retirement**

Currently, the State is facing a potential crisis due to the fact that over 27 percent of its full-time IT employees are eligible for retirement over the next five years. In addition, the State is constantly challenged with overall IT salaries historically being lower than in the private sector. And finally, due to budget constraints, much of the centralized training offerings have been either minimized or eliminated altogether. All of that said, the State has taken on several initiatives to improve recruiting and retention of IT employees over the past few years.

Although the data is from 2012, the ten largest agencies employ roughly 81 percent of the 1,474 full-time IT employees. On average, agencies have full-time IT staff that makes up approximately 6-7 percent of their total staff. As shown in the table below, although they are not the largest agencies, the Department of Revenue (DOR) and the Arizona Health Care Cost Containment System (AHCCCS), rely heavily on technology to provide services to their customers. Finally, the Arizona Department of Administration (ADOA) has the highest percentage of full-time IT employees due to the fact the ASET office, which is part of ADOA, acts as the central IT services broker for other agencies.

## IT Personnel

Agency	IT FTEs	Total FTEs	% IT FTEs	Eligible for Retirement*	% Eligible
Accountancy Board	2	23	8.70%	0	0.00%
AHCCCS	115	942	12.21%	38	33.04%
Arizona Commission on the Arts	1	12	8.33%	1	100%
Arizona Department of Racing	2	41	4.88%	0	0.00%
Attorney General	13	643	2.02%	4	30.77%
Banking Department	2	47	4.26%	0	0.00%
Building and Fire Safety	1	28	3.57%	0	0.00%
Corporation Commission	16	254	6.30%	2	12.50%
Cosmetology Board	1	24	4.17%	1	100%
Criminal Justice Commission	2	40	5.00%	0	0.00%
Department of Administration	143	584	24.49%	31	21.68%
Department of Agriculture	3	203	1.48%	1	33.33%
Department of Corrections	60	9029	0.66%	20	33.33%
Department of Economic Security	437	10360	4.22%	155	35.47%
Department of Education	48	599	8.01%	5	10.42%
Department of Environmental Quality	34	459	7.41%	15	44.12%
Department of Gaming	4	97	4.12%	1	25.00%
Department of Health Services	79	1650	4.79%	11	13.92%
Department of Housing	3	59	5.08%	0	0.00%
Department of Juvenile Corrections	4	559	0.72%	0	0.00%
Department of Real Estate	2	34	5.88%	0	0.00%
Department of Revenue	132	711	18.57%	39	29.55%
Department of Transportation	161	4211	3.82%	40	24.84%
Department of Weights and Measures	1	30	3.33%	0	0.00%

\*This represents the number of IT full-time employees who are eligible for retirement over the next five years.

IT Personnel

Agency	IT FTEs	Total FTEs	% IT FTEs	Eligible for Retirement*	% Eligible
Early Childhood Development	9	468	1.92%	1	11.11%
Forestry	2	124	1.61%	1	50.00%
Game and Fish Department	17	712	2.39%	2	11.76%
Geological Survey	6	42	14.29%	0	0.00%
Industrial Commission	7	243	2.88%	1	14.29%
Insurance Department	3	92	3.26%	1	33.33%
Land Department	24	129	18.60%	8	33.33%
Liquor Licenses Department	2	46	4.35%	1	50.00%
Lottery Commission	19	94	20.21%	7	36.84%
Medical Examiners Board	4	66	6.06%	0	0.00%
Military Affairs	21	480	4.38%	6	28.57%
Parks Board	5	287	1.74%	2	40.00%
Pharmacy Board	1	25	4.00%	0	0.00%
Power Authority	2	11	18.18%	1	50.00%
Registrar of Contractors	7	97	7.22%	3	42.86%
Retirement System	44	239	18.41%	4	9.09%
Secretary of State	11	151	7.28%	1	9.09%
State Board for School Capital Facilities	1	21	4.76%	0	0.00%
State Board of Nursing	2	69	2.90%	0	0.00%
State Treasurer	1	25	4.00%	0	0.00%
Structural Pest Control	2	17	11.76%	0	0.00%
Veterans Service Commission	4	430	0.93%	0	0.00%
Water Infrastructure Finance Authority	2	24	8.33%	0	0.00%
Water Resources	12	130	9.23%	3	25.00%

\*This represents the number of IT full-time employees who are eligible for retirement over the next five years.

As shown in the table above, almost one-third (27.54 percent) of the current 1,474 full-time IT employees will be eligible for retirement over the next five years. In addition, there are a handful of agencies that rely heavily on IT full-time employees, but also have a large percentage who are eligible for retirement. As an example, within the Department of Revenue, almost 20 percent of their full-time employees are in the IT department. Of those 132 employees, 39 of them (almost 30 percent) are eligible for retirement over the next five years. In addition, within the Arizona Health Care Cost Containment System (AHCCCS), roughly 12 percent of their full-time employees are in the IT department. Of those 115 employees, 38 of them (roughly 33 percent) are eligible for retirement over the next five years. To try and address some of these issues, in 2014, the State Human Resources office kicked off a marketing campaign to recruit and retain IT employees across all agencies.

Probably the most significant change the State has made in regards to IT personnel is the development of the new IT Classification System. In the past, all full-time IT resources were given a classification of an InfoTech Specialist #1 through #5. This system did not incorporate any standard IT job titles, descriptions, career paths, or salary ranges specific to industry-standard IT disciplines. In August 2014, the ADOA Human Resource (HR) division, in partnership with several agency CIOs, rolled out a new IT classification system for all state employees. In addition, the HR division completed a salary assessment after the employees were slotted into the new disciplines. This information was then shared with the agencies to address the salary discrepancies, assuming their budget would allow it.

The new standard disciplines established were:

- Application Development
- Business Analysis
- Change and Release Management
- Computer Systems Administration
- Database Administration
- Geographic Information Systems
- Help Desk / Service Desk
- Information Security
- Mainframe Operations
- Mainframe Systems Administration
- Project-Program Management
- Quality Assurance
- Supervisory-Management

More disciplines are continuing to be developed as deemed necessary by HR and the IT community. Going forward, a process has been established in which HR will engage ADOA-ASET if new disciplines need to be drafted.

### **IT Training Program**

In working with the Governor's office, ADOA-ASET implemented an IT Training Program to meet new IT skill requirements. The strategy is to provide training in a State facility, open participation to all agencies, and fill the class with as many participants as possible (largest class was a security class with 51 participants). Topics range from process improvement, business analysis, website development and administration, ITIL foundations, agile project management, enterprise architecture, database administration, security and service management.

The following is a list of the training classes:

- Defending Your Environment
- Drupal
- Web Application Security
- ITIL Foundations
- Agile PM
- Lean Concepts
- MySQL Administration
- Attacking Government Systems
- Building Secure Web Apps
- Defending Government Systems
- Defensive Programming—PHP and .Net
- How to Gather and Document Business Requirements
- Information Assurance Privacy and HIPAA
- Malware Analysis and Incident Response
- Defensive Programming—JAVA
- Establishing the Business Mindset for Technical Resources
- Managing Service Level Agreements
- Enterprise Architecture Refresher



The State just finalized the second year of this program with the following results:

Total Trainings



2013 - 6  
2014 - 13  
Total - 19

Total Participants



2013 - 248  
2014 - 347  
Total - 595

Total Training Hours



2013 - 152  
2014 - 312  
Total - 464

Total People Hours of Training



2013 - 6,312  
2014 - 8,088  
Total - 14,400

Total Training Cost



2013 - \$125,600  
2014 - \$199,653  
Total - \$325,253

Average Cost per Participant



2013 - \$506.45  
2014 - \$575.37  
Average - \$546.64

Average Cost of Training per Participant per Hour



2013 - \$19.90  
2014 - \$24.69  
Average - \$22.59

### **Centers of Excellence**

In addition to in-class training, through the Chief Information Officer (CIO) Council, The State has facilitated the creation of multiple Centers of Excellence (COEs) or IT working groups based on specific IT disciplines. Currently there are five COEs for Enterprise Architecture, Security, Privacy, Project Management and Business Analysts. There are several other COEs being evaluated such as Social Media, Application Development, Data Governance and Geographic Information Systems (GIS). Each COE consists of Subject Matter Experts (SMEs) from many state agencies, working together to achieve specific goals. These goals are defined by each COE in a charter. These goals range from monthly meetings to discuss key issues, developing tools and templates, drafting and reviewing policies, bringing in guest speakers, identifying training opportunities, creating development plans for employees within the discipline and many other items. The COEs also improve communication across state agencies at multiple organizational levels. A new portal for the statewide IT community is set to launch in the second quarter of FY 15.

### **Apprenticeship**

According to the Georgetown University Center on Education and the Workforce, by 2020, the United States is expected to face a shortage of 5 million workers<sup>42</sup> who are equipped with technical certificates and credentials. At the same time, about half of U.S. executives' at large companies say they are likely to have fewer skilled workers than they need in the next one to two years. Not surprisingly, employee retention is also a top concern for businesses that compete in the tightening market for skilled workers. Research has shown that apprenticeship offers myriad benefits to employers. By investing in talent development through apprenticeship, employers gain a pipeline of loyal skilled workers, increase productivity, and improve the bottom line.

#### **1. Build a pipeline of skilled workers**

Across the economy, employers worry about their rapidly aging workforces. For businesses faced with the increasing likelihood that they won't be able to rely solely on buying their talent, apprenticeship can be an effective tool to build their talent instead. In fact, more than 80 percent<sup>43</sup> of U.S. companies that sponsor apprentices say that apprenticeship is an effective strategy for helping them meet their demand for skilled labor.

<sup>42</sup><http://cew.georgetown.edu/recovery2020>

<sup>43</sup>[http://www.urban.org/Uploaded-PDF/411907\\_registered\\_apprenticeship.pdf](http://www.urban.org/Uploaded-PDF/411907_registered_apprenticeship.pdf)

**2. Gain workers with customized skills**

Through apprenticeship, businesses have the opportunity to train workers to meet their specific standards. In England, many companies that sponsor apprentices are realizing the benefits of a specialized workforce.

**3. Boost retention**

Apprentices are loyal to the companies that invest in them. Some employers may worry that other companies will hire away their new talent after they've made significant investments in their education and training. In England, the average retention rate for former apprentices—across all industries—is 73 percent. Moreover, a significant majority of apprenticeship sponsors report that apprenticeships actually raise productivity and worker morale across the board—not just among apprentices. This is because all workers benefit from a learning environment at work.

**4. Save money on wages**

Because apprentices start out earning about 40 percent to 50 percent less than a fully trained employee, businesses can save money on wages by sponsoring an apprentice. These lower wages serve to offset some of the costs of offering an apprenticeship program, which can include mentor time, equipment for training, and often tuition for classroom-based instruction. In the United Kingdom, a survey<sup>44</sup> of employers in four industries found that the productive value of apprentices ranged from 60 percent to 90 percent of their training costs—but companies at least broke even on their investment as a result of gains in post-apprenticeship productivity.

At a time when too many American workers lack the education and training to secure well-paying, middle-class jobs, and American businesses increasingly rely on high-skill workers to innovate and expand, we believe that apprenticeships hold great promise for addressing our nation's and state's economic challenges.

<sup>44</sup>[http://www2.warwick.ac.uk/fac/soc/ier/publications/2003/hogarth\\_and\\_hasluck\\_2003\\_rr418.pdf](http://www2.warwick.ac.uk/fac/soc/ier/publications/2003/hogarth_and_hasluck_2003_rr418.pdf)

<sup>45</sup>[http://www2.warwick.ac.uk/fac/soc/ier/publications/2003/hogarth\\_and\\_hasluck\\_2003\\_rr418.pdf](http://www2.warwick.ac.uk/fac/soc/ier/publications/2003/hogarth_and_hasluck_2003_rr418.pdf)

Apprenticeship is a time-tested approach to training and developing skilled labor. In the United States, a formal system of registered apprenticeship is administered by the U.S. Department of Labor<sup>45</sup>. Companies register their program with the department's Office of Apprenticeship, and, in return, the government issues a nationally recognized certificate to workers at the company who complete an apprenticeship. Apprenticeships can help meet the demand from businesses and the State should consider working closely with Arizona Commerce Authority and Western Apprenticeship Coordinators Association of Arizona (WACA) to create a statewide IT apprenticeship program and benefit from it.

# IT Government Funding



As of 2011, Oklahoma began implementing an agency-driven IT government model. House Bill 1170 was passed to create a State CIO position, which Oklahoma did not have previously, and to begin a major effort to consolidate IT. Since 2011, Oklahoma has made significant progress with its consolidation efforts.

In comparison, Arizona's first State CIO position was created in 2001. There has been a total of seven State CIOs since that time. In 2011, Arizona merged the Government Information Technology Agency (GITA), ADOA Information Services Division (ISD), and the Telecommunications Program Office (TPO) to form ADOA's Arizona Strategic Enterprise Technology (ASET) division. The consolidation increased alignment, governance, and shared services statewide. Although ADOA-ASET provides some level of shared services to nearly every agency, it is not a consolidated IT office.

Arizona has a robust project approval process that requires all IT projects with development (implementation) budgets \$25,000 and over to be approved by the State CIO. Additionally, all IT projects with development (implementation) budgets of \$1 million or more must be approved by the Information Technology Authorization Committee (ITAC). Any project funded through the Automation Projects Fund (APF) requires an additional "favorable review" from the Joint Legislative Budget Committee (JLBC). All projects over \$5 million must also engage a third-party for ongoing assessment services in order to help reduce project implementation risks.

ADOA-ASET is responsible for developing the Statewide IT Strategic Plan, as well as drafting and maintaining statewide IT Policies, Standards and Procedures (PSPs). Arizona maintains a very active Chief Information Officer (CIO) Council and IT community. Over the past two years, more than five statewide IT Centers of Excellence have been initiated in order to support specific IT disciplines. The State places a priority on championing strong governance, transparency and communication.

The State of Oklahoma has a decentralized IT budgeting model, and financed consolidation initiatives by means of a bond issuance. Arizona also has a decentralized IT budgeting model and is an area in which the State could see improvement. In 2012, Arizona created the strategic APF to enable specific transformation initiatives prioritized by the Governor. This helped to prioritize statewide budgets and resources aligning them to strategic, enterprise-wide IT projects.

### **Robust IT Governance**

Arizona has a track-record of more than thirteen years of strong IT governance. Founded in 2001, the Government Information Technology Agency (GITA), formed the first Arizona State CIO office. There have been seven CIOs since 2001, including the following:

- John Kelly
- Art Ranney
- Richard Zelznack
- Craig Stender
- Chris Cummiskey
- Chad Kirkpatrick
- Aaron V Sandeen

In July 2011, GITA merged with ADOA and the TPO, which was responsible for managing AZNet II. This merger formed a new division called ASET.<sup>46</sup>

ADOA-ASET is responsible for creating the statewide IT strategy, creating and maintaining Policies, Standards and Procedures (PSPs), approving all IT projects, and facilitating the ITAC. ADOA-ASET also holds monthly CIO Council meetings and has started more than five IT Centers of Excellence<sup>47</sup> focused on honing IT skills, growing the IT community, and sharing templates and tools.

### **Automation Project Fund (APF)**

IT budgeting and funding is federated within the individual agency. The APF was created to support a series of strategic transformation initiatives prioritized in the Governor's FY 13 budget plan, and finalized on May 7, 2012 by means of Laws 2012, 2nd Regular Session, Chapter 298, Section 1, which created A.R.S. § 41-714. As instituted, the APF:

<sup>46</sup><https://aset.az.gov>

<sup>47</sup><https://aset.az.gov/resources/centers-excellence>

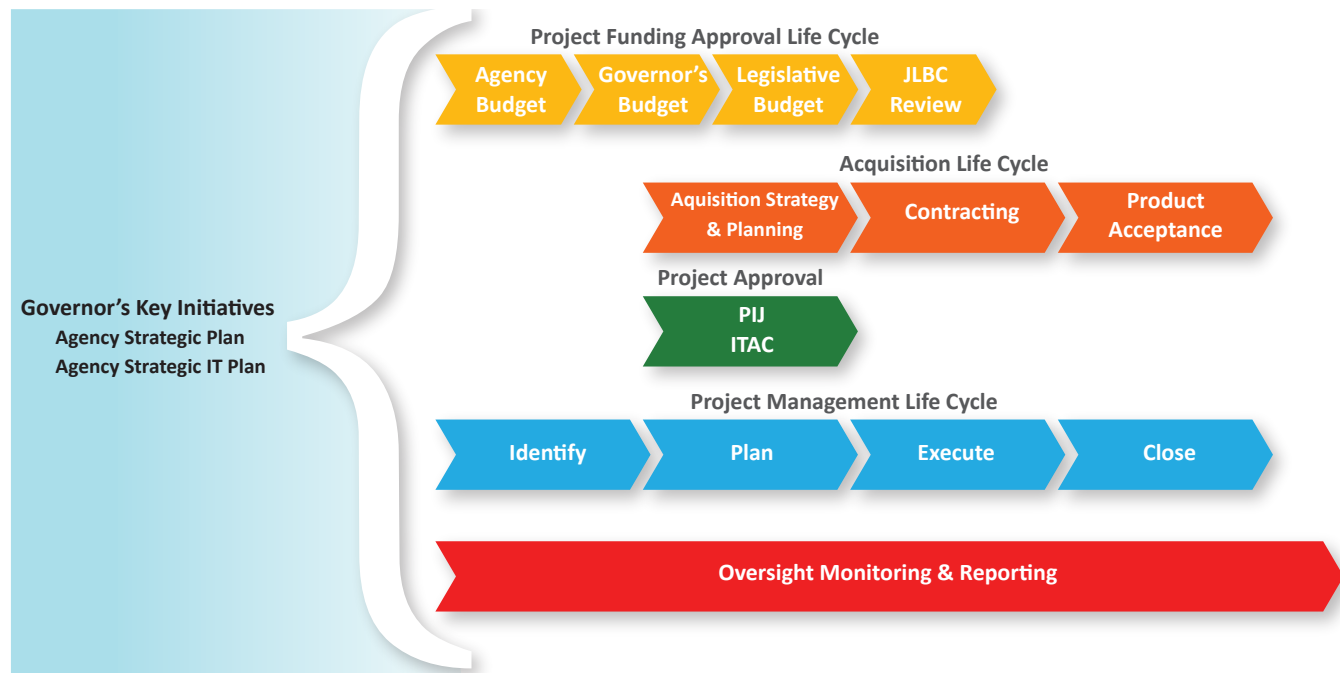
- Comprises monies appropriated by the legislature
- Mandates the Arizona Department of Administration (ADOA) as administrator of the fund
- Funding to be used to implement, upgrade, or maintain state agency automation and IT projects
- Requires Joint Legislative Budget Committee (JLBC) to favorably review the specific project expenditure plan for the fiscal year in which the monies are to be spent, prior to expenditure of any monies from the fund
- Requires ADOA to submit quarterly reports to JLBC on the implementation of APF funded projects, including the projects' deliverables, timeline for completion, expenses, and current status

This unique and effective project delivery and oversight methodology was developed to satisfy the critical demand for large-scale IT project funding required to address deferred maintenance and refresh the State's technology network and infrastructure. Under the direction of the Governor's Office and State CIO, a statewide IT management plan was developed and implemented in 2013. This plan proposed the consolidation of new and continuing IT projects with centralized oversight and project management provided by ADOA-ASET. All funding for these projects would pass through the new, non-reverting, APF.

As current legislation directs, APF monies are allocated to ADOA, which manages the funding utilized by individual agencies responsible for delivering specified IT projects. Favorable review by the JLBC is required prior to ADOA releasing funds and subsequent expenditure by the project-sponsoring agency. ADOA-ASET has defined the following APF – IT Project Life Cycle Framework, which provides guidance for the overall project life cycle by:

- Ensuring project sponsorship
- Defining the business problem(s) to be solved
- Identifying funding streams
- Developing and managing acquisition strategy
- Assuring compliance with the project approval process
- Executing the project and end-to-end monitoring and reporting

### Automation Projects Fund (APF) - IT Project Life Cycle Framework





In conjunction with this framework, State agencies are responsible for developing:

- Strategic IT plans aligned with the Governor’s key initiatives
- Budgets in consultation with the Office of Strategic Planning & Budgeting (OSPB) and the legislature
- Acquisition plans in alignment with the State Procurement Office (SPO)
- Project Investment Justification (PIJ) documentation
- Presentation of projects to the Information Technology Authorization Committee (ITAC), as required
- Efficient execution of projects and regular status reporting to ADOA-ASET

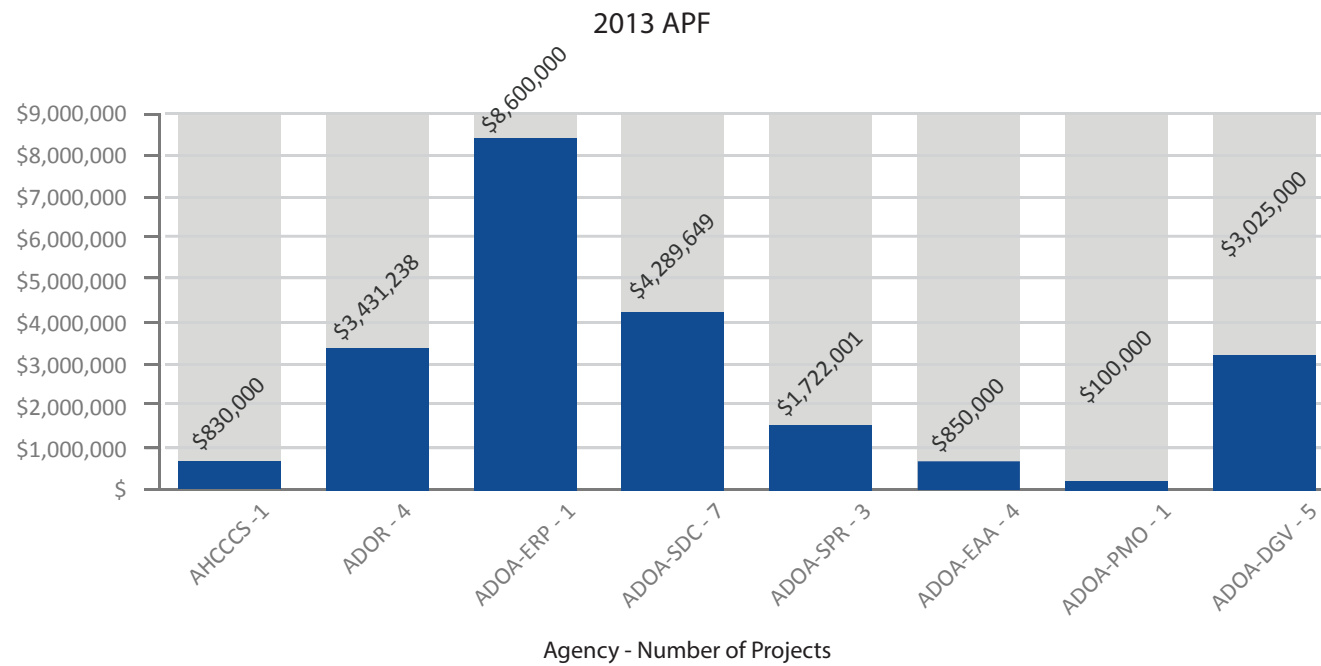
By law, agencies are mandated to work with ADOA-ASET to ensure APF funded IT projects are adhering to the State’s enterprise architecture framework, including applicable statewide policies and standards. The ADOA-ASET Strategic Oversight team assists agencies in navigating the PIJ and ITAC process for all APF project approvals. With the exception of non-PIJ (FTE and staff augmentation) projects, all APF funded projects require either State CIO (projects with development budgets under \$1 million) or ITAC (projects with development budgets of \$1 million or more) approval prior to JLBC review. ADOA-ASET also provides standards and best practices around project management and is responsible for end-to-end oversight and monthly PIJ status report monitoring.

ADOA utilizes ISAs to manage the APF funding process with project-sponsoring state agencies. This ISA process allows for transfer of APF funds through ADOA to the agency, and clarifies monthly reporting requirements, milestones, and other project related deliverables. Additional reporting requirements for APF projects, in addition to the standard Strategic Oversight Status Reports, include monthly Budget & Milestone Reports, which reflect project milestones and financial projections.

Examples of large-scale critical IT projects which have been, or are currently being, funded by the APF include:

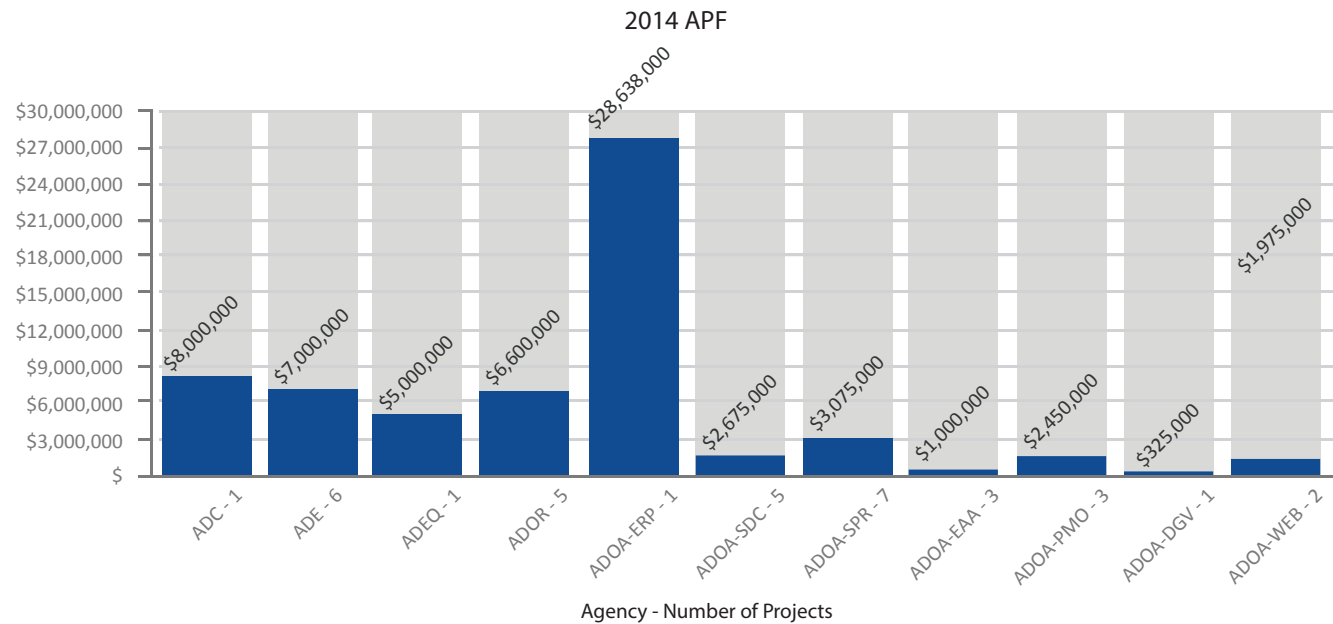
- Statewide accounting system
- Child Protective Services platform
- Department of Environmental Quality Permit and Licensing system
- Revenue Tax Collection system
- Department of Corrections Inmate Management system
- Statewide Network Security Management and Controls

The APF is now in its third year of existence. As illustrated below, in FY 13, the first year it was implemented, the APF included approximately \$23 million in funding for large-scale, high-risk IT projects. In FY 14, the amount increased to approximately \$67 million. For FY 15, APF appropriations include approximately \$70 million for new and continuing IT projects. Legislative appropriations through year three total approximately \$160,000,000.



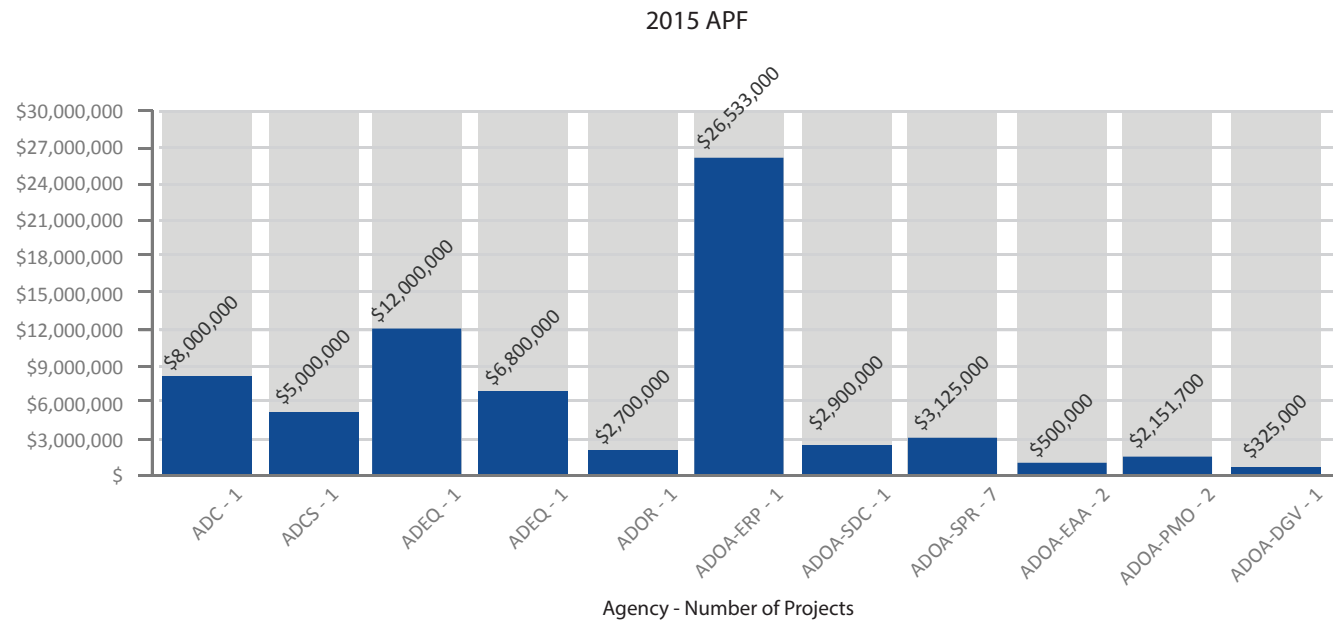
As illustrated above, three agencies were recipients of FY 13 APF funding appropriations totaling \$22,847,888, in support of 26 IT projects:

- Arizona Health Care Cost Containment System (AHCCCS) – 1 project
- Arizona Department of Revenue (ADOR) – 4 projects
- Arizona Department of Administration (ADOA) – 21 projects



As illustrated above, five agencies were recipients of FY 14 APF funding appropriations totaling \$66,738,000, in support of 35 new and continuing IT projects:

- Arizona Department of Corrections (ADC) – 1 project
- Arizona Department of Education (ADE) – 6 projects
- Arizona Department of Environmental Quality (ADEQ) – 1 project
- Arizona Department of Revenue (ADOR) – 5 projects
- Arizona Department of Administration (ADOA) – 22 projects



As illustrated above, six agencies were recipients of FY 15 APF funding appropriations totaling \$70,034,700, in support of 28 new and continuing IT projects:

- Arizona Department of Corrections (ADC) – 1 project
- Arizona Department of Child Services (ADCS) – 1 project
- Arizona Department of Education (ADE) – 9 projects
- Arizona Department of Environmental Quality (ADEQ) – 1 project
- Arizona Department of Revenue (ADOR) – 2 projects
- Arizona Department of Administration (ADOA) – 14 projects

The APF has proven to be a highly effective tool to drive large-scale IT initiatives and innovation throughout the State. With current funding and ongoing support from the Governor's Office and State legislature, this project delivery program will continue to benefit the State for years to come.

### **Federally Disallowed Expenditures**

The federal government often enlists state government as a partner through federal financial participation in a variety of programs. The federal government maintains equity shares in the funding streams and closely monitors the expenditure of enterprise fund activities. The programs are held to the formal federal standards dictated by 2 CFR 225 (The Federal Office of Management and Budgeting (OMB) A-87 Circular, Title 2 Code of Federal Regulations (CFR) part 225).<sup>48</sup>

The 2 CFR 225 identifies three types of cost activities that are specifically disallowed, and monies collected for disallowed purposes must be returned to the federal government. The amount to be returned is generally the total value of the disallowed amount multiplied by the proportion of all revenues in the fund derived from federal funding sources. This proportion is known as the Federal Financial Participation Rate (FFPR) and is calculated individually for each enterprise fund as some program activities accrue greater federal funding dollars than others. For example, the FFPR ranges from less than 2 percent in the State Surplus Materials Revolving Fund to over 37 percent in the Automation Operations Fund, which is a fund used by ADOA-ASET for delivering services to state agencies.

The following describes the disallowed purposes:

- **Disallowed Costs:** the Federal auditors will compare the program activities to the allowed activities in 2 CFR 225, and if it is determined that monies were expended on program activities outside of the allowed amounts, the disallowed amounts will be determined, the FFPR applied, and the resulting sum will be the determined refund amount.
- **Excess Retained Earnings:** enterprise funds will typically carry some balance beyond the annual

---

<sup>48</sup>[http://www.whitehouse.gov/sites/default/files/omb/fed-reg/2005/083105\\_a87.pdf](http://www.whitehouse.gov/sites/default/files/omb/fed-reg/2005/083105_a87.pdf)

needs of the fund. Carrying these balances is a good practice as it mitigates cash flow issues and provides some stability in funding demands should capital expenditures be needed or if contributing entities be subject to changes in the rates charged for services. Since there are a known proportion of federal monies in the revenue stream, federal auditors assume that the FFPR can be applied to the excess fund balance. 2 CFR 225 will allow a fund balance that is sufficient for 60 days working capital and for very specific other purposes relating to depreciation of equipment. The total fund balance amounts greater than the amounts allowed by 2 CFR 225 are known as Excess Retained Earnings (ERE); that amount, multiplied by the FFPR will be the determined refund amount. NOTE: Disallowed Costs themselves, by altering the allowable proportions of federal money in a fund, can recursively create additional ERE amounts.

- Fund Transfer Refunds: State policy makers will occasionally determine that the State portion of a fund balance has grown to the point where a portion can be transferred to the General Fund or some other fund. Depending on the amount of equity the State has in a fund, these state transfers may prompt a corresponding federal liability. If the state transfer amount is sufficiently large, the accrued federal liability may be in excess of the funds available.

In all cases, a federal refund accrued from an appropriated fund requires an appropriation. ADOA can provide language, similar to that of A.R.S. 41-750 (C.), which allows ADOA to refund monies without a defined amount appropriation.

The federal government conducts annual audits, which, due to the size of federal programs, occur on a consistent basis, with various programs and issues being audited at different times of the year. This complicates the budget request process as it is not possible to know at any given point in time exactly how much will be due to the federal government. The audit process involves some “negotiation”, which is more accurately understood as a complete exposition of the financial issues involved and the State’s interpretation of sometimes ambiguous financial events.

Refund amounts are formally conveyed to the State through a Determination Letter, which typically gives a (short) period of time to convey the refund to the appropriate Federal entity. Refund amounts accrue according to the terms of the Determination Letter.

This issue asks for a supplemental appropriation for amounts due in FY 14, and an appropriation for FY 15 for amounts that will be due in that fiscal year.

The following are examples of how this can impact IT:

- **Disallowed Costs:** The IT Fund in the ASET Division of ADOA is responsible for IT coordination, strategic planning, information security and privacy, and technology project oversight statewide. The Automation Operations Fund is used by ADOA-ASET to provide services for state agencies. Federal auditors determined that all costs associated with technology project oversight and large-scale capital investments are disallowed.
- **Excess Equity:** The Automation Operations Fund and IT Fund have been determined to have excess equity. Over the past three years, ADOA-ASET has transferred monies from these funds into the APF. Transferring these funds and completing projects out of the APF is a disallowed activity.
- **Fund Transfer Refunds:** Refunds from the IT Fund and the Telecommunications Fund (AZNet) have also been deemed disallowed.

Although this is not specifically a large-scale computing system issue, it absolutely impacts planning and acquisition of large-scale computer systems. ADOA-ASET has been working with the Arizona General Accounting Office (GAO) on this issue for several years. One strategy that is being deployed to avoid disallowed costs is the lease large-scale systems. ADOA-ASET is also working with the Arizona State Procurement Office (SPO) to ensure that the State has proper contracts to enable these types of purchases and to avoid disallowed cost issues.



Graphic icons made by Freepik,  
Icomoon, SimpleIcon, Yannick from  
<http://www.flaticon.com>



Arizona Department of Administration (ADOA)  
100 N. 15th Avenue, Phoenix Arizona, 85007  
Phone: 602-542-500 | Fax: 602-542-2199