



**ADOA - ASET**

Arizona Strategic Enterprise Technology

**Project Investment Justification**

**Version 01.01**

**A Statewide Standard Document for Information Technology Projects**

**Project Title:**

**Centralized Cloud Security Management**

<b>Agency Name:</b>	Arizona Department of Administration
<b>Date:</b>	November 15, 2013
<b>Agency Contact Name:</b>	Mike Lettman
<b>Agency Contact Phone:</b>	
<b>Agency Contact Email:</b>	

[Hover for Instructions](#)

## I. Management Summary\*

In Fiscal Year 2014 (FY14), a number of transformation initiatives were prioritized by Governor Janice K. Brewer, proposed in her budget, and subsequently codified into law. Included in these initiatives are a series of measures designed to further protect the State from the ever-increasing threats to its systems and data from a wide range of internal and external sources.

The Arizona Department of Administration's Arizona Strategic Enterprise Technology Office (ADOA-ASET) has adopted a "Cloud First" strategy for migrating applications and service offerings from the State Data Center (SDC) to vendor-hosted computer networks, also known as the "cloud." As more service offerings are moved to the cloud, ADOA-ASET must ensure that Federal Risk and Authorization Management Program (FedRAMP) and National Institute of Standards and Technology (NIST) security controls are in place to provide the appropriate levels of protection for State applications and data. In this project, leading-edge technologies will be researched, selected, and implemented to establish recommended levels of security in the cloud environment.

## II. Project Investment Justification (PIJ) Type\*

Yes  No Is this document being provided for a Pre-PIJ / Assessment phase?

If Yes,

Identify any cost to be incurred during the Assessment phase.	\$
Based on research done to date, provide a high-level estimate or range of development costs anticipated for the full PIJ.	\$

Explain:

Yes  No Will a Request for Proposal (RFP) be issued as part of the Pre-PIJ or PIJ?

## III. Business Case

### A. **Business Problem\***

In order to support the "Cloud First" strategy for migrating applications and service offerings to the cloud environment, additional security measures are required. Because technology is rapidly evolving, research is needed to understand what cloud security options are available to protect State data and applications. ADOA-ASET is also looking to migrate security-related management services to a vendor-hosted cloud environment.

### B. **Proposed Business Solution\***

In alignment with strategic goals, ADOA-ASET will research options and acquire cost-effective solutions to protect and manage applications and data as they are migrated to the cloud. In addition to security protections and management services, this project will also ensure business continuity for those applications and service offerings migrated to the cloud. Solutions to be addressed include:

**Cloud Application Protections**

ADOA-ASET will research technologies and select vendors that follow FedRAMP guidelines and provide NIST-recommended security controls in the cloud environment. These technologies include cloud security proxy services to protect State web applications from malicious attacks, cloud encryption and firewall protections to secure data from external threats, and cloud content filtering to protect users from malicious internet content.

**Cloud Security Management Services**

Based on services and technology already in use, ADOA-ASET will enable business continuity and provide security management functions with the migration of supporting services to the cloud. These services include remote desktop access, secure file transfer, configuration management, network authentication and authorization, directory access, Internet Protocol (IP) address assignments, and domain name services.

**C. Quantified Benefits\***

<input checked="" type="checkbox"/>	Service enhancement
<input type="checkbox"/>	Increased revenue
<input checked="" type="checkbox"/>	Cost reduction
<input checked="" type="checkbox"/>	Problem avoidance
<input checked="" type="checkbox"/>	Risk avoidance

Explain:

This project will enhance services, reduce costs, avoid problems, and mitigate risks by:

- Providing additional security protections
- Implementing technology solutions with improved sustainability
- Bringing continuity, flexibility, and reliability to cloud-based business services
- Implementing equivalent security for service offerings migrated to the cloud

**IV. Technology Approach**

**A. Proposed Technology Solution\***

ADOA-ASET will evaluate and select vendors capable of providing cloud-based security services and will also acquire vendor-hosted services to provide security-related management in the cloud.

**Cloud Application Protections**

ADOA-ASET will select vendors capable of providing technologies that meet the defined security requirements within vendor-hosted cloud environments. Costs in the PIJ include a three (3) year up-front license for specific application protections to be implemented in the cloud. The proposed technology solutions will be evaluated for renewal or replacement prior to the end of the three (3) year period. These technologies include:

- **Cloud Security Proxy Services** – providing an additional layer of security by blocking malicious external attacks to State web applications and systems.

- **Cloud Encryption and Firewall Protections** – securing cloud data by controlling, analyzing, and blocking malicious web traffic.
- **Cloud Content Filtering** – protecting users and systems by blocking access to web sites that may contain malicious or objectionable content.

### **Cloud Security Management Services**

Based on the SDC infrastructure in place and options available, this solution will migrate security related services to the vendor-hosted cloud environment. This approach will also enhance business continuity through robust, cloud-based service capabilities. Costs in the PIJ include the initial year of security management services; ongoing costs for this initiative are already included in current operational expenses for the technology being migrated. Security management services to be provisioned in the cloud include:

- **Remote Desktop Services** – providing a secure method to access State networks from a remote location.
- **Secure File Transfer Services** – allowing employees to send, receive, and store files securely.
- **Configuration Management Software** – providing remote access control, re-imaging of desktops remotely, and distributing application, anti-virus protection, and operating system updates.
- **Active Directory Controllers** – managing authentication and authorization for all users and computers on the network.
- **Lightweight Directory Access Protocol** – providing a mechanism for accessing and maintaining directory information from servers.
- **Dynamic Host Configuration Protocol** – allowing devices (e.g., computers and printers) to be configured for network communication using assigned IP addresses.
- **Internal Domain Name Services (DNS)** – translating a web address to an IP address, thereby allowing a user or application to connect to a specific online destination.

## ***B. Technology Environment***

Although some of the proposed technologies exist in some State agencies, including ADOA, current implementations may not support the FY14 “Cloud First” initiative. While implemented initially for ADOA, these technologies are expected to provide the foundation for cost-effective implementations within other State agencies.

## ***c. Selection Process***

The Security, Privacy and Risk team within ADOA-ASET (ASET/SPR) is proposing to acquire technologies through the following processes:

### Cloud Application Protections

Working in partnership with State agency leadership, ADOA-ASET will identify business needs and security gaps, and subsequently select a group of cloud technologies from the Gartner Magic Quadrant®. Leading Magic Quadrant® vendors on State contract will be asked to provide demonstrations of their proposed solutions to help further define business requirements and selection criteria. Gartner is an established research and advisory firm that produces qualitative analysis and performance information about technologies currently available in the marketplace.

Upon review of the available options and costs, the State's Chief Information Security Officer (CISO) will recommend solutions to the State Chief Information Officer (CIO) for approval. Once approved, deployment will be based on the cloud environment security requirements.

### Cloud Security Management Services

Vendor-hosted services will be acquired based on the specific technologies to be migrated into the cloud. Professional contract support services will also be acquired to assist with the configuration and migration into production.

## V. Project Approach

### A. Project Schedule\*

Project Start Date: 12/02/13      Project End Date: 6/30/14

### B. Project Milestones

Major Milestones	Start Date	Finish Date
<b>Cloud Application Protections:</b>		
Magic Quadrant® vendors on State contract identified	2/03/14	3/28/14
Vendor products demonstrated and requirements established	3/31/14	5/16/14
Bid process completed and vendor selected	2/10/14	5/31/14
Solutions determined by CISO	3/10/14	3/28/14
Vendor selection presented by CISO to CIO and approval received	3/31/14	4/11/14
Specific vendor technologies acquired	4/14/14	6/13/14
<b>Cloud Security Management Services:</b>		
Vendor solutions selected	1/06/14	1/31/14
Solutions purchased from vendors on State contract	2/03/14	3/31/14
Vendor resources acquired for set-up and migration	2/03/14	3/31/14
Solutions moved to production	4/01/14	6/30/14

## VI. Roles and Responsibilities

### A. Project Roles and Responsibilities

**Agency Director:** Brian C. McNeil, ADOA Director

**Agency Chief Information Office (CIO):** Aaron V. Sandeen, ADOA Deputy Director, State CIO

**Project Sponsor:** Mike Lettman, Chief Information Security Officer (CISO), ADOA-ASET

**Project Manager:** Nancy Brister, Project Manager, ADOA-ASET

**Enterprise Capabilities and Delivery Coordination:** David Nale, Project Manager, ADOA-ASET  
**Technical Project Manager:** Hector Virgen, Information Security Manager, ADOA-ASET  
**Cloud Application Protections Technical Lead:** Jennifer Dvorak, Networking Analyst, ADOA-ASET  
**Cloud Security Management Technical Lead:** Jared Clarke, Networking Analyst, ADOA-ASET

**NOTE:** Above individuals may be replaced with group members with equivalent skill set.

**B. Project Manager Certification**

- Project Management Professional (PMP) Certified
- State of Arizona Certified
- Project Management Certification not required

**C. Full-Time Employee (FTE) Project Hours**

<b>Total Full-Time Employee Hours</b>	1920
<b>Total Full-Time Employee Cost</b>	\$

**VII. Risk Matrix, Areas of Impact, Itemized List, PIJ Financials**

## VIII. Project Approvals

### A. Agency CIO Review\*

Key Management Information	Yes	No
1. Is this project for a mission-critical application system?	X	
2. Is this project referenced in your agency's Strategic IT Plan?	X	
3. Is this project in compliance with all agency and State standards and policies for network, security, platform, software/application, and/or data/information as defined in <a href="http://aset.azdoa.gov/security/policies-standards-and-procedures">http://aset.azdoa.gov/security/policies-standards-and-procedures</a> , and applicable to this project? If <b>NO</b> , explain in detail in the "XI. Additional Information" section below.	X	
4. Will this project transmit, store, or process sensitive, confidential or Personally Identifiable Information (PII) data? If <b>YES</b> , in the "XI. Additional Information" section below, describe what security controls are being put in place to protect the data.	X	
5. Is this project in compliance with the Arizona Revised Statutes (A.R.S.) and GRRC rules?	X	
6. Is this project in compliance with the statewide policy regarding the accessibility to equipment and information technology for citizens with disabilities?	X	

### B. Project Values\*

The following table should be populated with summary information from other sections of the PIJ.

Description	Section	Number or Cost
Assessment Cost (if applicable for Pre-PIJ)	II. PIJ Type - Pre-PIJ Assessment Cost	\$
Total Development Cost	VII. PIJ Financials tab	\$650,000
Total Project Cost	VII. PIJ Financials tab	\$650,000
FTE Hours	VI. Roles and Responsibilities	1920

### C. Agency Approvals\*

Contact	Printed Name	Signature	Email and Phone
Project Manager:	Nancy Brister		
Agency Information Security Officer:	Mike Lettman		
Agency CIO:	Aaron V. Sandeen		
Project Sponsor:	Mike Lettman		
Agency Director:	Brian C. McNeil		

## IX. Optional Attachments

### A. *Vendor Quotes*

## X. Glossary

## XI. Additional Information

This project is specifically intended to provide appropriate levels of protection for PII data that may reside in the cloud.

Links:

[ADOA-ASET Website](#)

[ADOA-ASET Project Investment Justification Information Templates and Contacts](#)

Email Addresses:

[Strategic Oversight](#)

[ADOA-ASET\\_Webmaster@azdoa.gov](mailto:ADOA-ASET_Webmaster@azdoa.gov)