



ADOA - ASET

Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title:

Data Center Network Managing and Monitoring

Agency Name:	ADOA-ASET
Date:	October 22, 2013
Agency Contact Name:	Mike Lettman
Agency Contact Phone	
Agency Contact Email:	

[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 the initiatives are a series of measures designed to further protect the State against the ever-increasing threats to its systems and data from a wide range of internal and external sources.

In support of these objectives, the Arizona Department of Administration's Arizona Strategic Enterprise Technology Office (ADOA-ASET) will utilize security assessment information collected in FY13 to analyze and prioritize critical firewall security gaps within the State. In partnership with other State agencies, ADOA-ASET will also research and evaluate firewall technologies currently available in the marketplace. With the information gathered as part of this initiative, a comprehensive firewall solution will be selected and implemented to address identified security gaps.

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***

While assessment data collected in FY13 identified security vulnerabilities in a subset of State systems and web applications, additional information is needed regarding the firewall capabilities currently in place across the State. Firewall technologies, which are used to restrict or prevent potentially malicious network traffic, have continued to evolve. However, information regarding where and how these are being used is lacking. In order to assess and address potentially critical gaps in firewall protections, ADOA-ASET will identify and partner with State agencies with similar security needs that:

- Lack this technology, thereby exposing the Agency and interconnected State systems to potential risks
- Require more current or advanced technology capable of providing more secure protections
- Have implemented firewall solutions with high maintenance costs and sustainability issues
- Require life cycle replacement to avoid product malfunctions

B. **Proposed Business Solution***

In alignment with ADOA-ASET's strategic goals, this project will identify currently available firewall technologies that can further protect the State from external threats to its systems and

data. Implementation of comprehensive and up-to-date firewall security devices and software will provide ADOA and other State agencies with additional protective barriers against malicious internet traffic and unauthorized access.

Key efforts of this project will include an analysis of current State agency firewall protections to identify and prioritize security gaps, as well as research and selection of leading edge or “next-generation” firewall technologies capable of addressing those gaps. With the information gathered, ADOA-ASET will propose specific implementations of selected firewall protections, where feasible and most cost-effective for the State.

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:

- Adding firewall technology that is not currently in place
- Reducing future maintenance, support, and life cycle replacement costs
- Implementing advanced cyberattack detection and prevention capabilities offered by next-generation firewall technologies

IV. Technology Approach

A. Proposed Technology Solution*

ADOA-ASET will evaluate and select vendors capable of providing a comprehensive suite of leading edge firewall technologies that can meet the wide-ranging security needs across the State. These technologies provide active monitoring and filtering capabilities that can restrict internet traffic based on content.

While the selected tools will be implemented initially within the ADOA environment, they are expected to offer a standardized and cost-effective solution for other State data centers that may require firewall protection. Costs in this PIJ reflect the acquisition of firewall hardware devices, also known as “appliances,” as well as licensing for the selected vendor’s software suite, including maintenance and support for two (2) additional years.

The breakdown of costs is based on limited research conducted by ADOA-ASET and partner agencies regarding these technologies, as well as the likely number of implementations that can be accommodated with available funding. The proposed solution will be re-evaluated for renewal or replacement with new technology prior to the end of the three (3) year period.

B. Technology Environment

Although firewall technologies exist within the ADOA environment, some of these may need to be replaced with next-generation firewall technologies to provide appropriate levels of security

control. In other State data centers, firewall protections are likely to be lacking or outdated, which presents potential security risks throughout State systems and web applications. The selected firewall technologies will need to be integrated into the established data center environments.

C. Selection Process

The Security, Privacy and Risk team within ADOA-ASET (ASET/SPR) will work in partnership with State agency leadership to identify business needs and security gaps, and subsequently select a group of firewall technologies that can help to address those gaps based on the Gartner Magic Quadrant.® Leading Magic Quadrant® vendors that are on State contract will be asked to provide demonstrations of their proposed solutions to help further define business requirements and selection criteria. Gartner is a respected 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 a single vendor’s solution to the State Chief Information Officer (CIO) for further consideration and approval. Once approved, deployment will be determined based on a prioritization of security risks that can be addressed within the project’s budget and time constraints.

V. Project Approach

A. Project Schedule*

Project Start Date: 11/04/13 **Project End Date:** 6/13/14

B. Project Milestones

Major Milestones	Start Date	Finish Date
Initial gap analysis conducted	11/04/13	12/31/13
Magic Quadrant® vendors on State contract identified	11/04/13	12/31/13
Vendor products demonstrated and requirements established	1/06/14	2/07/14
Bid process completed and vendor selected	2/10/14	3/07/14
State leadership collaboration and solution 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 purchased and deployed	4/14/14	6/13/14

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

Technical Project Manager: Hector Virgen, Information Security Manager, ADOA-ASET

Firewalls Implementation Lead: Ken Dworshak, 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

Total Full-Time Employee Hours	250
Total Full-Time Employee Cost	\$

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 http://aset.azdoa.gov/security/policies-standards-and-procedures , and applicable to this project? If NO , 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 YES , 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	\$499,805
Total Project Cost	VII. PIJ Financials tab	\$499,805
FTE Hours	VI. Roles and Responsibilities	250

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

Links:

[ADOA-ASET Website](#)

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

Email Addresses:

[Strategic Oversight](#)

ADOA-ASET_Webmaster@azdoa.gov