Janice K. Brewer
Governor

Brian C. McNeil
Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 NORTH FIFTEENTH AVENUE • SUITE 401
PHOENIX, ARIZONA 85007

(602) 542-1500

August 14, 2014

Mr. Brian C. McNeil, Director
Arizona Department of Administration
100 N. 15th Ave.
Phoenix, AZ 85007

Dear Brian:

In response to the *Amended* Project Investment Justification (PIJ) for the **"Data Center Network Managing and Monitoring"** project, my staff has reviewed your proposal to acquire and implement leading edge technologies to provide additional firewall protections for the State.

The original PIJ implied funding was available from the Fiscal Year 2014 (FY14) Automation Projects Fund (APF) in the amount of $499.8 thousand for the total three-year life cycle cost of the project. The amended PIJ implies additional funding is available from the FY15 APF for a total four-year life cycle cost for the project of $1,015.0 thousand.

This is notification of Arizona Strategic Enterprise Technology Office's recommendation to the Information Technology Authorization Committee (ITAC) for **Approval with Conditions** of the *Amended* technology project as follows:

1. Should there be a change in the proposed costs of 10% or more, the Security, Privacy and Risk (SPR) team within ADOA-ASET must amend the PIJ to reflect the changes and present it to ITAC for review and approval prior to further expenditure of funds.

The ITAC is scheduled to meet on August 27, 2014 to review this project. Should the ITAC approve the project, you may then proceed to secure additional approvals as required from the Joint Legislative Budget Committee, the Office of Strategic Planning and Budgeting, and the State Procurement Office.

Best Wishes,

Aaron V. Sandeen
State CIO and Deputy Director
Arizona Strategic Enterprise Technology (ASET) Office

jc

cc: Mike Lettman, ADOA-ASET
        Nancy Brister, ADOA-ASET

Andrew Smith, JLBC
John Arnold, OSPB
Barbara Corella, SPO
Phil Manfredi, ADOA-ASET
Jeffrey Crane, ADOA-ASET

ASET# AD14007_A

Agency Name & Address	Contact Name & Phone
Arizona Department of Administration 100 N. 15th Ave. Phoenix, AZ 85007	Mike Lettman 602-542-0030 Mike.Lettman@azdoa.gov
Project and Investment Justification Name	Date Submitted
Data Center Network Managing and Monitoring	November 8, 2013 (original date) *August 8, 2014* (amended date)

Project Overview

Problem Description

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 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. While assessment data collected in FY13 by the Arizona Strategic Enterprise Technology (ASET) Office within the Arizona Department of Administration (ADOA) identified security vulnerabilities in a subset of State systems and web applications, additional information is needed regarding where and how existing firewalls are being used across the State. Designed to restrict or prevent potentially malicious network traffic, firewalls have continued to evolve, with more advanced "next-generation" technologies able to provide active monitoring and filtering capabilities that can restrict internet traffic based on content. While the current ADOA environment may require some next-generation firewall technology, to provide additional levels of security controls, firewall protections are likely to be lacking or outdated in other State data centers, which presents potential security risks throughout State systems and web applications.

Solution

In alignment with strategic goals, ADOA-ASET is proposing to 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, in order to identify and select leading edge next-generation firewall technologies capable of addressing identified security gaps. Once a comprehensive firewall solution has been selected, ADOA-ASET will propose specific implementations of the selected firewall protections into established data center environments, where feasible and most cost-effective for the State.

In FY14, ADOA identified and partnered with State agencies to research, evaluate, and define firewall security protection requirements, and awarded a Next Generation Firewall (NGFW) solution contract. These efforts resulted in ADOA, State agencies, and other governmental entities having a firewall solution and standard to consider for purchase through an awarded contract and negotiated rates. In FY15, ADOA is proposing to utilize remaining FY14 and new FY15 Automation Projects Fund (APF) monies to implement the NGFW solution for ADOA and to partner with other State agencies to expand NGFW protections.

Measurements and Deliverables

In order to assess and address potentially critical gaps in firewall protections, the Security, Privacy and Risk team within ADOA-ASET (ASET/SPR) 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

Once business needs and security gaps have been identified, a group of firewall technologies that can help to address those gaps will be selected, based on 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. Based on this analysis, ADOA-ASET will evaluate vendor options for acquiring a comprehensive suite of leading edge firewall technologies that can meet the wide-ranging security needs across the State. 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, ADOA-ASET will propose specific implementations for deployment based on a prioritization of security risks and requirements.

Development costs reflect an estimated number of firewall security devices or "appliances," as well as licensing for the selected vendor's software suite, including maintenance and support for two (2) additional years. Pending final selection, costs are based on 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.

In FY15, ADOA proposes to complete the purchase, installation, and implementation of the NGFW solution for ADOA and to partner with other State agencies across the enterprise to expand NGFW protections. Specific milestones include:

- *Purchase, plan, and implement NGFW solution in ADOA*
- *Evaluate and prioritize additional agencies requiring expanded NGFW solutions*
- *Acquire and implement NGFW solution in selected State agencies and/or entities*

The project will require an end date extension, to allow time to acquire and implement the solutions.

Benefits

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. The proposed project is expected to 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

The expansion of the original project scope will allow ADOA to implement NGFW technology that will increase data security and help prevent external and internal threats to the ADOA network. Additionally, by partnering with other State agencies, ADOA will help prevent these threats where protections currently do not exist.

Project Management

The ADOA-ASET Project Manager will work with ASET/SPR subject matter experts and participating State agencies to complete the project deliverables.

Enterprise Architecture

Compliant.

Original Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	499.8	0.0	0.0	0.0	0.0	499.8
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	499.8	0.0	0.0	0.0	0.0	499.8

Amended Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	499.8	515.2	0.0	0.0	0.0	1,015.0
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	499.8	515.2	0.0	0.0	0.0	1,015.0

Recommendation: Approval with Conditions

1. Should there be a change in the proposed costs of 10% or more, the Security, Privacy and Risk (SPR) team within ADOA-ASET must amend the PIJ to reflect the changes and present it to ITAC for review and approval prior to further expenditure of funds.