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 **"FY14 Security Assessments"** project, my staff has reviewed your proposal to continue efforts to address security risks through additional penetration testing, vulnerability assessments, and mitigation of FY14 findings.

The original PIJ implied funding was available from the Automation Projects Fund (APF) in the amount of $450.0 thousand for the total five-year life cycle cost of the project. The amended PIJ implies additional funding is available from the Fiscal Year 2015 (FY15) APF in the amount of $590.0 thousand, for a total five-year life cycle cost for the project of $1,040.0 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# AD14001_A

Analyst: Jeffrey Crane **PIJ Summary - ASET** Project Number: AD14001_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*
FY14 Security Assessments	August 9, 2013 (original date) ***August 6, 2014*** (amended date)

Project Overview

Problem Description

In Fiscal Year 2014 (FY14), a number of transformation initiatives were prioritized by Governor Janice K. Brewer in her plan, "The Four Cornerstones of Reform," 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 confidential data. While a number of security protection and risk mitigation measures were successfully implemented in FY13 by the Arizona Strategic Enterprise Technology (ASET) Office within the Arizona Department of Administration (ADOA), the State must continue to understand, evaluate and mitigate its security risks. The growing threats and attempts from cybercriminals to steal confidential data from computer systems are well documented and continue to come from a variety of internal and external sources. The State of Arizona's many web applications and the State Data Center (SDC) represent prime targets to cybercriminals due to the large amount of potentially profitable data collected. The prior SDC security assessment conducted under PIJ AD13009, and penetration testing of ten (10) mission-critical web applications conducted under PIJ AD13010, were foundational efforts that helped to identify the State's current risk exposure to potential threats. There are many other web applications, however, as well as a number of other State data center facilities currently operating independently of the SDC, which could be facing similar risks.

Solution

To further address security risks to the State, ADOA is proposing to build upon the completed FY13 security initiatives by conducting penetration testing on a second set of ten (10) mission-critical web applications, and also performing security assessments for up to six (6) State agency data centers. Working in collaboration with other State agencies, ADOA will utilize an independent third-party vendor on State contract to identify potential targets, and assess and prioritize weaknesses that may be found. The resulting information and recommendations can then be used to correct high-risk vulnerabilities and identify areas for further investigation and remediation. Additional resources will be acquired from CAaNES and/or other vendors on State contract, as applicable, to complete this work.

During FY14, ADOA completed security assessments of identified mission-critical State applications and data centers. This included retesting for remediation of FY13 identified risks. During FY15, ADOA will continue to utilize security assessment data to analyze and address critical firewall security gaps and further mitigate risks within the State.

Measurements and Deliverables

ADOA is proposing to partner with other State agencies to continue to build upon previous risk mitigation efforts in the following key areas:

- Penetration testing for approximately ten (10) additional State web applications
- Independent data center assessments and mitigation for up to six (6) State agencies

Given the success of the previous efforts, ADOA plans to once again utilize CAaNES as an independent third-party vendor to provide the professional services to execute the testing and assessments. As a subcontractor available through CenturyLink, the State's voice and network communications provider, CAaNES demonstrated the subject matter expertise and sensitivity required to successfully complete the FY13 security efforts. Findings and recommendations provided by CAaNES will be summarized in a set of reports which will allow each participating agency to understand their specific risk exposure while also providing ADOA management with a better view into the security risk profile for the State.

This expansion of the original project scope will allow ADOA to accomplish the following:

- ***Annual penetration testing for additional mission-critical State applications***
- ***Vulnerability assessments against approximately 10,000 Internet Protocol (IP) addresses***
- ***Retesting of applications mitigated as a result of FY14 security assessments***
- ***Address new vulnerabilities and security problems identified through additional security assessments***

ADOA plans to once again utilize CAaNES as an independent third-party vendor to provide the professional services to execute the testing and assessments. The project will require an end date extension, to allow time to acquire and implement the solutions.

Benefits

This project is designed to identify security risks through penetration testing of additional State web applications, and also to identify and address vulnerabilities in other data center facilities operating within the State. Unless adequately protected, applications running in the SDC and other facilities can provide cybercriminals with an easy means to steal great amounts of data with significant financial value. The impact of such a data breach can include disruption of business capabilities, punitive fines by regulatory bodies, loss of public confidence and good will, and extensive remediation costs. The FY13 security projects were well-received and valued by the agencies involved, and were successful in providing management with useful information about the State's cybersecurity risk profile. The FY14 initiatives are expected to further efforts to address potential gaps that could result in a data breach.

These added security assessments and associated tasks will provide critical data to assist the State in the identification and mitigation of security gaps and vulnerability issues associated with mission critical applications and systems.

Project Management

The ADOA-ASET Enterprise Project Management Office (EPMO) Project Manager will work with Subject Matter Experts from the ADOA-ASET Security, Privacy and Risk (SPR) team to acquire the vendor services, identify and coordinate testing and assessment activities with participating agencies, and complete required deliverables.

Enterprise Architecture

Compliant.

Original Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	450.0	0.0	0.0	0.0	0.0	450.0
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	450.0	0.0	0.0	0.0	0.0	450.0

Amended Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	450.0	590.0	0.0	0.0	0.0	1,040.0
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	450.0	590.0	0.0	0.0	0.0	1,040.0

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.