ADOA-ASET

Arizona Strategic Enterprise Technology

Project Investment Justification
(PIJ)

A Statewide Standard
Document for Information Technology Projects

Project Title: ***FY14 Security Assessments***

Agency Name: ***ADOA-ASET***
Date: ***August 5, 2013***
Prepared By: ***Nancy Brister***

Revised PIJ Version – January 2013

TABLE OF CONTENTS

I. General Information

I.A General Information {A}

Agency CIO:	Aaron V. Sandeen	**Contact Phone:**	602-364-4770
Agency Contact Name:	Mike Lettman	**Contact Phone:**	602-542-0030
Agency Contact Email:	Mike.Lettman@azdoa.gov	**Prepared Date:**	August 2, 2013

I.B Special Funding Considerations {A}

☐ **Yes** ☒ **No - Does this project require funding approved for a Pre-PIJ Assessment phase?**

If **YES**, provide details for the **Pre-PIJ Assessment** funding needs by filling out the areas marked with **{A}** or **{Required for Pre-PIJ Assessment only}**. Further information and details will be required after the assessment for final PIJ approval.

If **NO**, provide details for the final PIJ by filling out **all** areas **excluding** those sections marked with **{Required for Pre-PIJ Assessment only}**.

II. Project Overview

II.A Management Summary {A}

I. 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." Included in the initiatives proposed in her budget, and finalized by the legislature in Laws 2013, 1st Special Session, Chapter 1, Section 115, are a series of measures designed to further protect the State against the ever-increasing threats to its systems and confidential data from a wide range of internal and external sources. While a number of security protection and risk mitigation measures were successfully implemented in FY13 by the Arizona Strategic Enterprise Technology Office within the Arizona Department of Administration (ADOA-ASET), the State must continue to understand and evaluate its security risks, in order to determine how best to protect State information.

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. Recent findings from the independent security assessment, conducted under prior PIJ AD13009, helped to identify the SDC's current risk exposure to potential threats. However, there are a number of independent data center facilities around the State which could be facing similar risks that also require evaluation and mitigation. While the penetration testing that was conducted for ten (10) mission-critical web applications, under prior PIJ AD13010, was successful in identifying potential risks associated with those specific applications, there are many other web applications in the State that could present similar risks.

II. Solution

The Security, Privacy and Risk team within ADOA-ASET (ASET/SPR) proposes 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

III. Quantified Justification

This project is designed to identify security risks through penetration testing of selected web applications and to identify and address vulnerabilities in other State data center facilities. 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.

II.B Existing Situation and Problem, "As Is" {A}

While the projects implemented in FY13 by the ASET/SPR team have made the State more secure, assessments conducted in FY13 also made it clear that Arizona remains at risk from the growing threats and attempts from cybercriminals to steal confidential data. The State has many web applications to serve its citizens that could potentially be compromised due to the lack of proper security controls. In addition to the SDC, a number of independent data center facilities around the State are running these web applications, which can make those facilities a target for data theft as well.

II.C Proposed Changes and Objectives, "To Be" {A}

ADOA-ASET is proposing to partner with other State agencies to continue to build upon the completed FY13 security initiatives. These efforts were well-received and valued by the involved agencies, and were successful in providing management with useful information about the State's cybersecurity risk profile. Areas of focus in FY14 include:

- **Mission-Critical Applications Penetration Testing** - Acquire services from an independent third-party vendor on State contract to test for vulnerabilities in a second set of ten (10) mission-critical web applications.

- **Mitigation of Vulnerability Assessment** - Acquire services from an independent third-party vendor on State contract to perform data center assessments for up to six (6) State agencies. Contract resources will also be utilized to address vulnerabilities that have been identified.

III. Project Approach

III.A Proposed Technology {Required for PIJ Approval}

ADOA-ASET proposes using an independent third-party vendor, CAaNES, to provide the professional services to conduct the penetration testing and vulnerability assessments. CAaNES demonstrated the subject matter expertise, experience, and ability to achieve the desired results in regard to the prior security assessment services contract. Additional resources may be acquired from CAaNES and/or through other vendors on State contract to complete system configuration changes needed to mitigate identified vulnerabilities.

III.B Other Alternatives Considered

While ADOA-ASET considered utilizing other vendors for the security assessment and testing services, CAaNES was chosen based on the sensitivity and success demonstrated by the FY13 efforts. Given the security risks, continuing to find ways to identify and protect the State against potential threats has proven to be a valuable approach.

III.C Major Deliverables and Outcomes

1. Joint Legislative Budget Committee (JLBC) Favorable Review received

2. Agency participation solicited and determined for additional penetration testing
3. Agency contacts for coordination of security assessments identified
4. Security assessment and testing contract(s) finalized
5. Assessment requirements, methodology and approach finalized
6. Application and agency contact information provided to vendor
7. Penetration testing on each of the ten (10) web applications coordinated, scheduled, and executed
8. Security assessments for up to six (6) State agency data centers completed
9. Vendor results reviewed with individual agencies
10. Executive summary reports and recommendations presented
11. Overall results and remediation recommendations for participating agencies completed
12. Mitigation efforts to resolve high risk security issues identified and implemented

IV. Policies, Standards and Procedures

IV.A Enterprise Architecture

☒ **Yes** ☐ **No -** Does this project meet all 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?

If **NO,** please describe ***NEW*** or ***EXCEPTIONS*** to Standards {Network, Security, Platform, Software/Application and/or Data/Information}:

IV.B Service-Oriented Architecture Planning and Implementation

☐ **Yes** ☒ **No -** Does this project qualify as an SOA application by improving application delivery for technology reuse and/or application reuse and/or services reuse?

IV.C Disaster Recovery Plan and Business Continuity Plan

☐ **Yes** ☒ **No -** Does this project require a Disaster Recovery Plan and Business Continuity Plan?

IV.D Project Operations

☐ **Yes** ☒ **No -** Is there a written assessment of short-term and long-term effects the project will have on operations?

IV.E Web Development Initiative

☐ **Yes** ☒ **No -** Is this a Web Development initiative? If **YES**, a Notice of Intent (**NOI**) must be provided. Link: http://aset.azdoa.gov/node/15

IV.F State IT Goals

Please check which goal the project is in support of; if more than one, indicate the primary goal.

☐ Accelerate Statewide Enterprise Architecture Adoption
☐ Champion Governance, Transparency and Communication
☐ Invest in Core Enterprise Capabilities
☒ Proactively Manage Enterprise Risk
☐ Implement a Continuous Improvement Culture
☐ Adopt Innovative Sustainability Models
☐ Reduce Total Cost of Ownership
☐ Improve Quality, Capacity and Velocity of Business Services
☐ Strengthen Statewide Program and Project Management
☐ Build Innovative and Engaged Teams
☐ Other_____

V. Roles and Responsibilities

V.A Project Roles and Responsibilities

Please identify project roles and responsibilities:

Agency Director: Brian C. McNeil, ADOA Director
Agency CIO: Aaron V. Sandeen, ADOA Deputy Director, State Chief Information Officer (CIO)
Project Sponsor: Mike Lettman, ADOA-ASET Chief Information Security Officer (CISO)
Project Manager: Nancy Brister, Project Manager, ADOA-ASET
Technical Project Manager: Hector Virgen, Information Security Manager, ADOA-ASET
System Administrator(s): Jared Clarke, Network Analyst, Team Lead, ADOA-ASET

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

Project Management:

ADOA-ASET/SPR Subject Matter Experts
- Complete requirements definition and planning activities
- Create purchasing requirements and finalize vendor contract(s)
- Identify stakeholders
- Develop Implementation and Communication Plan
- Oversee coordination of vendor activities with identified agencies
- Manage vendor and staff resources related to this project
- Provide progress, status, and issues to management

ADOA-ASET Enterprise Project Management Office (EPMO)
- Facilitate monitoring overall project status
- Identify and assist with competing project priorities, as needed

Please indicate Project Manager (PM) certification:

The **project manager** assigned to the project is:

☒ Project Management Professional (PMP) certified
☐ State of Arizona certified
☐ PM certification not required

VI. Project Benefits

VI.A Benefits to the State

Score: **0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive**

Description	*Score*
Agency Performance: The extent to which duties and processes will improve or positively affect business functions. Consider reduced redundancy and improved consistency for the agency.	3
Productivity Increase: The improvements in quantity or timeliness of services or deliverables. Consider improved turnaround time or expanded capacity of key processes.	1
Operational Efficiency: Efficiencies based on improved use of resources, greater flexibility in agency responses to stakeholder requests, reduction or elimination of paperwork, legacy systems, or manual tasks.	2
Accomplishment Probability: The extent to which this project is expected to have a high level of success in completing all requirements for the division or agency.	4
Functional Integration: The impact the project will have in eliminating redundancy or improve consistency. Consider the impact of information sharing between departments, divisions, or agencies in the State.	1
Technology Sensitive: The implementation of the right types of technology to meet clear and defined goals and to support key functions. Consider technologies and systems already proven within the agency, division, or other similar organizations.	3
Total	14
Additional Information *(provide details on scores > 3)*	
Describe additional details on scores > 3. Also provide details on any savings that may be applicable. The **Accomplishment Probability** score is based on the success of the foundational efforts in FY13.	

VI.B Value to the Public

Score: **0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive**

Description	*Score*
Client Satisfaction: Rate how stakeholders may respond to anticipated improvements. This could apply to health and welfare services, quality of life or life safety functions.	3
Customer Service: Rate anticipated improvements to internal and external customer service delivery. Give consideration to faster response, greater access to information, elimination or reduction in client complaints.	2
Life Safety Functions: Applies to public protection, health, environment, and safety. Consider how this project will reduce risk in these functions.	1
Public Service Functions: Applies to licensing, maintenance, payments, and tax. Consider how this project will enhance services in these functions.	1
Legal Requirements: Consideration should be given to projects mandated by federal or state law. Other consideration could be given if there are interfaces with other federal, state, or local entities.	3
Total	10
Additional Information *(provide details on scores > 3)*	
Describe additional details on scores > 3.	

VII. Project Timeline {A}

VII.A Project Schedule

Provide <u>estimated</u> schedule for the development of this project. These dates are estimates only; more detailed dates will be required at project start-up once the project schedule is established.

Project Start Date: 8/21/13 **Project End Date:** 6/30/14

VIII. Project Financials

Project Funding Details Select One ☐ **Pre-PIJ Assessment Funding Details Only**
☒ **Full PIJ Project Funding Details**

VIII.A Pre-Assessment Project Financials {Required for Pre-Assessment PIJ Only}

Project Funding Details for Pre-Assessment Project Investment Justification Only

(Double click on table below – add funding in **whole dollars** and then click outside the table to return to Word)

ESTIMATED COSTS						
Category	*FY2014*	*FY2015*	*FY2016*	*FY2017*	*FY2018*	*Total*
Assessment Costs						$ -
Development Costs						$ -
Total Development Costs (including Assessment)	$ -	$ -	$ -	$ -	$ -	$ -
Operational Costs (if estimate is available)						$ -
Total Estimated Project Costs	$ -	$ -	$ -	$ -	$ -	$ -

VIII.B Detailed Project Financials {Required for PIJ Approval}

Development and Operational Project Funding Details

Funding Categories:

Professional & Outside Services: *The dollars to be expended for all third-party consultants and contractors.*
Hardware: *All costs related to computer hardware and peripheral purchases for the project.*
Software: *All costs related to applications and systems related software purchases for the project.*
Communications: *All costs related to telecommunications equipment, e.g., switches, routers, leased lines, etc.*
Facilities: *All costs related to improvements or expansions of existing facilities required to support this project.*
License & Maintenance Fees: *All licensing and maintenance fees that might apply to hardware, software and any other products as up-front costs to the project (ongoing costs would be included under operational expense).*
Other: *Other IT costs not included above, such as travel, training, documentation, etc.*
NOTE*: FTE costs may be included in section VIII.E below, as required.*

(Double click on table below – add funding in whole dollars and then click outside the table to return to Word)

DEVELOPMENT COSTS						
Category	*FY2014*	*FY2015*	*FY2016*	*FY2017*	*FY2018*	*Total*
Professional & Outside Services	$ 450,000					$ 450,000
Hardware						$ -
Software						$ -
Communications						$ -
Facilities						$ -
License & Maintenance Fees						$ -
Other						$ -
Total Development Costs	$ 450,000	$ -	$ -	$ -	$ -	$ 450,000

Enter Total Development Costs (above) in Project Values table on Approvals page.

OPERATIONAL COSTS						
Category	*FY2014*	*FY2015*	*FY2016*	*FY2017*	*FY2018*	*Total*
Professional & Outside Services						$ -
Hardware						$ -
Software						$ -
Communications						$ -
Facilities						$ -
License & Maintenance Fees						$ -
Other						$ -
Total Operational Costs	$ -	$ -	$ -	$ -	$ -	$ -

Enter Total Project Costs (below) in Project Values table on Approvals page.

TOTAL COSTS						
	FY2014	*FY2015*	*FY2016*	*FY2017*	*FY2018*	*Total**
TOTAL PROJECT COSTS * Includes development and operational costs	$ 450,000	$ -	$ -	$ -	$ -	$ 450,000

VIII.C Funding Source {A}

(Double click on table below – add funding in **whole dollars** and then click outside the table to return to Word)

Funding Source Category	Name of Funding Source	Currently Available ($)		New Request ($)		Total ($)
		Development Budget	Operational Budget	Development Budget	Operational Budget	
General Fund						$ -
Federal ARRA Fund						$ -
Federal Fund						$ -
Other Appropriated Funds	Automation Projects Fund	$ 450,000				$ 450,000
Other Non-Appropriated Funds						$ -
TOTAL PROJECT COSTS (Should = development and operational totals above)		$ 450,000	$ -	$ -	$ -	$ 450,000

VIII.D Special Terms and Conditions (if required) {A}

Special Terms and Conditions (if required)
NA

VIII.E Full-Time Employee Project (FTE) Hours

Provide estimated FTE Development hours that will be utilized for the duration of the project. Include IT as well as Business Unit FTE hours, if available. Enter into Project Values table on Approvals page. **Enter FTE costs (if known) as well.**

Total Full-Time Employee Hours	100
Total Full-Time Employee Cost	$

IX. Project Classification and Risk Assessment

IX.A Project Classification and Risk Assessment Matrix

Rate each question to determine risk level at Low (0), Medium (1), High (2), Very High (3).

Enter Risk Score into Project Values table on Approvals page.

RISK EVALUATION RANGES	
LOW RISK PROJECT	0 - 8
MEDIUM RISK PROJECT	9 - 25
HIGH RISK PROJECT	26 - 42
VERY HIGH RISK PROJECT	43 +

Add Project Risk Details (if required)

PIJ Project Classification and Risk Evaluation					
Risk Factor	**Low (0)**	**Medium (1)**	**High (2)**	**Very High (3)**	**Score**
Project Management Complexity					
Project Team Size (# of people)	1-5	6-10	11-15	> 15	1
Project Manager (PM) Experience	Deep experience in this type of project	Some experience in this type of project and able to leverage subject matter experts	Some experience in this type of project and has limited support from subject matter experts	New to this type of project	0
Team Member Availability	Dedicated staff for project activities only as assigned	Staff is in place, few interruptions for non-project tasks are expected and have been accounted for	Available, some turnover expected, some interruptions for non-project issues likely	Dedicated team not available, staff will be assigned based on capacity	1
Number of Agencies Involved in Development Activity	1	2	3	> 3	1
Vendor (if used)	No vendor required	Vendor has been used previously with success	Vendor has been used previously with some management support required	New vendor and/or multiple vendors	1
Project Schedule	Schedule is flexible	Schedule can handle minor variations, but deadlines are somewhat firm	Scope or budget can handle minor variations, but deadlines are firm	Scope, budget and deadlines are fixed and cannot be changed	0
Project Scope	Scope is defined and approved	Scope is defined and pending approval	Scope being defined	High-level definition only at this point	0
Budget Constraints	Funds allocated	Funds pending approval	Allocation of funds in doubt or subject to change without notice	No funding allocated	1
Project Methodology	Defined methodology	Defined methodology, no templates	High-level methodology framework only	No formal methodology	0
IT Solution Complexity					
Product Maturity (if purchased)	Product implemented & working in > 1 agency or business of similar size	Product implemented & working in 1 agency or business of similar size	Product implemented & working only in an agency or business of smaller size	Product not implemented in any agency or business	0
Solution Dependencies	No dependencies or interrelated projects	Some minor dependencies or interrelated projects but considered low risk	Some major dependencies or interrelated projects but considered medium risk	Major high-risk dependencies or interrelated projects	0
System Interface Profile	No other system interfaces	1-2 required interfaces	3-4 required interfaces	> 4 required interfaces	1
IT Architectural Impact	Follows State IT approved design principles, practices & standards	New to the State, but follows established industry standards	Evolving "industry standard"	No standards, leading edge technology	0
Deployment Impact					
Process Impact	No business process changes	Agency-wide process changes	Multi-agency process changes	Statewide process changes	1
Scope of End User Impact	Department or division level only	Multiple division or agency-wide impacts	Multi-agency impacts	Statewide impacts	1
Training Impact	No training is required	Minimal training is required	Considerable training is required	Extensive training is required	1
				Total Risk Score	**9**

X. Project Approvals

X.A CIO Review {A}

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 consistent with agency and State policies, standards and procedures?	X	
4. Is this project in compliance with the Arizona Revised Statutes and GRRC rules?	X	
5. Is this project in compliance with the statewide policy regarding the Accessibility to Equipment and Information Technology for Citizens with Disabilities?	X	
6. Is this project mandated by law, court case or rule? If yes, cite the federal requirement, A.R.S. reference or court case. Details: *Provide details related to technology as part of the requirement.*		X

X.B Project Values

The following table contains summary information taken from the other sections of the PIJ document.

Description	Section	Significance
Assessment Costs *{A)*	VIII. Project Financials **{Required for Pre-Assessment PIJ Approval Only}**	$
Economic Benefits	VI. Benefits to the State	14
Value Rating	VI. Value to the Public	10
Total Development Costs	VIII. Project Financials	$450,000
Total Project Costs	VIII. Project Financials	$450,000
FTE Hours	VIII. Project Financials	100
Project Risk Factors	IX. Risk Summary	9

X.C Project Approvals {A}

Select One ☐ **Pre-PIJ Assessment Approval Only** ☒ **PIJ Project Approval**

Project Title: FY14 Security Assessments

Responsibility	*Printed Name*	*Approval Signature*	*Date*
Project Manager:	Nancy Brister		8/5/13
Agency CIO:	Aaron V. Sandeen		8.6.13
Project Sponsor:	Mike Lettman		8/5/13
Agency Director:	Brian C. McNeil		9 AUG 2013

Appendix

A. Itemized List with Costs

Assessment	Service Description	Cost
Penetration Testing	Services to perform in-depth manual and automated vulnerability testing on ten (10) identified State web applications.	$175,000
Mitigation of Vulnerability Assessments	Assessment and mitigation services for six (6) State agency data centers related to security vulnerabilities from inside and outside the respective networks.	$275,000
	Total Costs:	**$450,000**

B. Connectivity Diagram

NA

C. Project Schedule - Gantt Chart or Project Management Timeline

NA

D. NOI (Web Projects Only)

NA

Glossary

Document Information

Title:	Project Investment Justification – PIJ Version January 2013
Originator:	Arizona Department of Administration – AZ Strategic Enterprise Technology Office
Date:	January 2013
Download:	http://aset.azdoa.gov/
Contacts:	**ASET Oversight Managers:** http://aset.azdoa.gov/content/project-investment-justification **Web Design (NOI Contact):** http://aset.azdoa.gov/webtools