ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title:

Secure Data Protection Pilots

Agency Name:	**ADOA-ASET**
Date:	**October 1, 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.

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 build upon these strategic efforts. For this initiative, ADOA-ASET will evaluate and implement two (2) key technologies designed to provide additional layers of protection from unauthorized access and data theft.

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**

Currently, ADOA-ASET does not have technologies in place to identify the location of sensitive data across State systems or to defend against capabilities that can be utilized by cybercriminals to gain unauthorized access to that data. Knowing where sensitive data resides is a first line of defense against the theft or "exfiltration" of that data. Once the location of sensitive data is identified, additional security protections can be put in place to help prevent the unauthorized access of that data.

*B. Proposed Business Solution**

In alignment with ADOA-ASET's strategic goals, this project will address potential data threats through additional layers of security controls. Two (2) leading-edge technologies are proposed as security measures designed to identify and protect sensitive data from unauthorized access:

- A Data Loss Prevention (DLP) solution will allow the State to identify and track the location of sensitive data (e.g., Personally Identifiable Information (PII)) as an initial step toward preventing the exfiltration of that data.

- Multi-factor Authentication helps prevent sensitive data from being compromised by ensuring that user access to a system housing that data requires two (2) or more levels of authentication. For example, the authentication involves something the user must know, such as a password, along with something the user must have, such as a special file or a key fob, to gain access.

*C. Quantified Benefits**

	Service enhancement
	Increased revenue
	Cost reduction
X	Problem avoidance
X	Risk avoidance

Explain:

This project is designed to identify and mitigate security risks by adding layers of security controls to protect against unauthorized access to State systems containing sensitive data, thereby preventing data theft or breaches.

IV. Technology Approach

*A. Proposed Technology Solution**

ADOA-ASET will evaluate and select vendors capable of providing DLP and Multi-factor Authentication protection for State systems. These vendor tools will be implemented initially within the ADOA environment, and are expected to provide the foundation for cost-effective implementations within other State agencies in the next fiscal year.

The proposed solution includes a dedicated server for each of the technologies to house the specialized software and the large volumes of data that will be generated. Also, a security appliance, to monitor the network for data loss, has been included as part of the DLP solution. Estimated costs in the Itemized List section are based on research conducted regarding these technologies.

B. Technology Environment

These proposed technologies are not in use within the ADOA environment. The selected solutions, however, will need to integrate into the existing ADOA and other State agency computing environments.

C. Selection Process

ADOA-ASET is proposing to research and pilot both the DLP and Multi-factor Authentication technologies within the ADOA environment initially, in anticipation of additional pilots for other State agencies. The Security, Privacy and Risk team within ADOA-ASET (ASET/SPR) will work with participating State agencies to select the group of vendor technologies to pilot, based on the Gartner Magic Quadrant.® Gartner, Inc., a respected research and advisory firm, produces qualitative analysis and performance information about technologies currently available in the marketplace to support client decision-making. Leading Magic Quadrant® vendors that are on

State contract will be selected to provide demonstrations of their proposed solutions, which are expected to help further define business requirements and selection criteria.

In partnership with State agency leadership, ASET/SPR will follow the process captured in the "Project Milestones" section below, for each of the proposed technologies. Vendors under consideration will be asked to provide initial and final bids for implementing their respective solutions. Based on the technology approach and the cost-effectiveness of the vendor proposals, the State's Chief Information Security Officer (CISO) will recommend both a DLP and a Multi-factor Authentication solution for further consideration and approval by the State CIO. Prior to committing to their use, ASET/SPR will conduct a subsequent proof-of-concept (POC) to confirm the viability of each solution in the ADOA environment.

V. Project Approach

*A. Project Schedule**

Project Start Date: 11/11/2013 **Project End Date**: 6/20/2014

B. Project Milestones

Major Milestones	Start Date	Finish Date
Magic Quadrant® vendors identified	11/11/13	2/21/14
Vendor products demonstrated and requirements established	1/06/14	2/21/14
Bid process completed and vendor solutions selected	2/24/14	3/31/14
Solutions recommended and CIO approval received	4/01/14	4/18/14
POC conducted on selected solutions	4/21/14	5/31/14
Solutions purchased and installed	6/01/14	6/20/14

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
DLP Implementation Lead: Ed Yeargain, Compliance Analyst, ADOA-ASET
Multi-factor Authentication Implementation Lead: Chad Tom, IT Security, ADOA-ASET

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

B. Project Manager Certification

- [X] 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	300
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	$349,809.00
Total Project Cost	VII. PIJ Financials tab	$349,809.00
FTE Hours	VI. Roles and Responsibilities	300

C. *Agency Approvals**

Contact	Printed Name	Signature	Email and Phone
Project Manager:	Nancy Brister		
Agency Security Officer (CISO):	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 will provide specific security controls to help prevent access and exfiltration of sensitive data, including PII, which already resides in State agency computing environments.

Links:

ADOA-ASET Website

ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:

Strategic Oversight

ADOA-ASET_Webmaster@azdoa.gov