ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title:

Data Center Security Management

Agency Name:	**ADOA-ASET**
Date:	**September 24, 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 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 build upon these efforts. The FY13 *Strengthen Cyber Security Operations* transformation initiative successfully deployed technologies in the State Data Center (SDC) to automate threat management and implement intrusion detection system (IDS) functionality. For this FY14 initiative, ADOA-ASET will enhance its ability to identify attacks, data compromises, and data theft; ensure compliance; and expand protections to include other State of Arizona data centers.

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 the projects implemented in FY13 enhanced security in the SDC, ADOA-ASET needs to further protect State data from cybersecurity threats that may be directed toward other State agency data centers that lack intrusion detection capabilities. Additional security layers are needed to integrate information generated from multiple sources into consolidated, centralized reporting for ADOA-ASET and other State agencies. This approach will enhance incident detection and response and will help ensure compliance with security policies and standards.

*B. Proposed Business Solution**

In alignment with ADOA-ASET strategic goals, this project will address potential threats through expanded monitoring of State internet connections, more sophisticated analytics technology, and additional automated compliance capabilities. Security Operations Center (SOC) subject matter experts (SMEs) will be utilized to further evaluate and report on information generated from the proposed technologies.

*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 enhancing monitoring and compliance throughout the State. The proposed solution will integrate new and existing technologies within the SDC and other State agency data centers in order to expand cybersecurity threat identification and improve responses to cyberattacks.

IV. Technology Approach

*A. Proposed Technology Solution**

ADOA-ASET will conduct a proof-of-concept (POC) of a new compliance and analysis tool, to be offered by an existing vendor partner on State contract. This analysis tool will correlate data from a variety of other individual tools to create a dashboard of the current cybersecurity threat situation. In addition, the tool will use the same input to identify regulatory compliance issues and security gaps.

A dedicated server will be required to house the compliance and analysis software and data that will be generated during the expected three (3) year life of the product. Ancillary software tools will be acquired to allow specific data streams to be analyzed, which may include web applications, servers, laptops/desktops, network switches and firewalls. ADOA-ASET will determine which tools are needed based on monitoring requirements and cost. In addition to SDC devices and applications, input from other agency applications can be consolidated, correlated, and analyzed by this tool.

ADOA-ASET will also contract with the U.S. Department of Homeland Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) for monitoring and alert services. MS-ISAC services are currently used to monitor internet communications and receive alerts regarding potential threats for one (1) internet access point. However, additional devices are required to monitor traffic across additional internet access points.

B. Technology Environment

While the SDC is a central hub for much of the data processing and network communication across the State, many agencies currently operate their own data centers which may be at additional risk for cybersecurity threats. By acquiring the proposed solution, ADOA-ASET will be able to integrate information from other data feeds and intrusion detection systems, thereby providing a consolidated view into potential SDC and other State data center cybersecurity threats.

C. Selection Process

Based on previous demonstrations by vendors available on State contract, ADOA-ASET is proposing to conduct an initial POC of the new compliance and analysis software in anticipation of a full-scale implementation. ADOA-ASET will evaluate and select, based on value and cost, the ancillary tools that are capable of feeding the compliance and analysis software in order to determine applicable use. ADOA-ASET will consider whether the proposed solution will be renewed and/or replaced with new technology at the end of the three (3) year period.

MS-ISAC services are already in use, providing a high value to the State. Additional services will be purchased to monitor two (2) additional internet access points. After three (3) years, ADOA-ASET will establish either a billable service for sustainability or drop the service.

V. Project Approach

*A. Project Schedule**

Project Start Date: 10/30/2013 **Project End Date**: 6/30/2014

B. Project Milestones

Major Milestones	Start Date	Finish Date
Purchase server and onboard SOC contractors	11/01/13	11/15/13
Perform POC on compliance and analysis software	11/18/13	12/31/13
Identify required ancillary compliance monitoring tools	11/18/13	12/31/13
Implement compliance software and monitoring tools	1/06/14	5/30/14
Operationalize expanded compliance monitoring capabilities	6/01/14	6/30/14
Acquire MS-ISAC expanded services and connection devices	1/06/14	5/30/14
Verify internet access points monitoring by MS-ISAC	6/01/14	6/30/14
Operationalize expanded MS-ISAC alerts	6/01/14	6/30/14

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

System Administrator(s): Ken Dworshak, Network Analyst, Team Lead, 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	150
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	**$710,943**
Total Project Cost	VII. PIJ Financials tab	**$710,943**
FTE Hours	VI. Roles and Responsibilities	**150**

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

Links:

ADOA-ASET Website

ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:

Strategic Oversight

ADOA-ASET_Webmaster@azdoa.gov