



# ADOA - ASET

Arizona Strategic Enterprise Technology

## Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

**Project Title: ASRS Security Enhancements**

<b>Agency Name:</b>	Arizona State Retirement System
<b>Date:</b>	12/9/2014
<b>Agency Contact Name:</b>	Molly Mahai
<b>Agency Contact Phone:</b>	
<b>Agency Contact Email:</b>	

[Hover for Instructions](#)

## I. Management Summary\*

In January 2014, ASRS participated in an external Security Assessment conducted . The report included recommendations to further secure our network and mature our security program. The State defined security policies recommend some of the same solutions that the security assessment recommended.

While a number of security protections and risk mitigation measures were successfully implemented in the last year, ASRS must continue to build upon these strategic efforts and mature our security program. For this initiative, ASRS will evaluate and implement three (3) key technologies designed to provide additional layers of protection from unauthorized access and data theft which include next generation firewalls, data loss prevention and multi-factor authentication.

## 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\*

ASRS has firewalls that are approaching end of life and do not have the advanced technology capable of providing more secure protections. Additionally, ASRS does not have adequate technologies to prevent the unauthorized access of that data. Adding multi-factor authentication provides additional protection against unauthorized access.

### B. Proposed Business Solution\*

In alignment with our strategic goals, this project will address potential data threats through additional layers of security controls. Three (3) leading-edge technologies are proposed as security measures designed to identify and protect sensitive data from unauthorized access:

- Implementation of a next generation firewall will provide the ASRS with additional protective barriers against malicious internet traffic and unauthorized access.
- A Data Loss Prevention (DLP) solution will allow ASRS 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. Our solution needs to include perimeter as well as end point protection.

- 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 key fob, to gain access.

**C. Quantified Benefits\***

<input checked="" type="checkbox"/>	Service enhancement
<input type="checkbox"/>	Increased revenue
<input type="checkbox"/>	Cost reduction
<input checked="" type="checkbox"/>	Problem avoidance
<input checked="" type="checkbox"/>	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\***

The proposed solution includes two (2) physical next generation firewall appliances from Palo Alto, a security appliance for the DLP and possibly agents for the endpoints, and a soft token solution from Microsoft for multi-factor authentication.

**B. Technology Environment**

The proposed solutions are not currently used at the ASRS but must integrate with our existing infrastructure. Our current infrastructure consists of Firewalls which will be replaced by solution. We have a Cisco switch connected to physical servers and virtual server clusters. We will be migrating to VPN with the solution along with the multi-factor authentication. The data loss prevention tool must be able to protect the perimeter as well as endpoints.

We are not concerned about the technology fitting in with our architecture since we have vetted the solutions and all are compatible with our current technology infrastructure. We will also be verifying all the components of the solution before we purchase.

**C. Selection Process**

ASRS reviewed the agreements established by ADOA to determine if we could benefit from the same solution. For the solutions: next generation firewall, DLP, and multi-factor authentication, we plan to use the ADOA agreements where they fit into our architecture.

**Next Generation Firewall**

We participated in the research conducted by ADOA during their project and learned of the features from potential vendors. Out of that research, we looked at [redacted] and [redacted] since we already had [redacted] products, we considered them as well. We compared cost and features along with required skillset for setup and maintenance. While the [redacted] model had the required features with a reasonable cost, it required significant skills in Cisco products to configure and maintain. The [redacted] had the same features with additional visibility into the application layer and a much easier learning curve. The solution is also scalable for future growth. We chose the [redacted] solution utilizing the purchasing mechanism established by ADOA.

**Data Loss Prevention**

Rather than duplicate efforts already made by ADOA, we elected to take advantage of the procurement option they created. After completing research for the solution, we have allocated a budget amount for this endeavor and will engage with the vendor selected by the ADOA RFP process.

**Multi-Factor Authentication**

We looked at two options including a USB key provided by [redacted]. The solution must integrate with the VPN, multi-factor features available on the Next Generation firewall as well. It was determined fairly quickly that a physical key would be more costly and harder to manage than a software solution. A software solution proved much more feasible and we chose [redacted]. We are currently investigating whether we can use the service provided by ADOA or if we need to purchase through our own agreement. This will depend on how the solution integrates into our architecture. The numbers in the itemized spreadsheet correspond to our own solution.

**V. Project Approach**

**A. Project Schedule\***

**Project Start Date:** 1/12/2015      **Project End Date:** 6/30/2017

**B. Project Milestones**

Major Milestones	Start Date	Finish Date
Procure Firewalls	1/12/2015	1/26/2015
Receive Firewalls	3/2/2015	3/2/2015
Install/Configure Firewalls	3/2/2015	6/2/2015
Procure multi-factor solution	7/6/2015	7/20/2015
Implement multi-factor solution	7/20/2015	12/31/2015
Procure Data Loss Prevention Tool	1/4/2016	1/18/2016
Implement Data Loss Prevention Tool	1/19/2016	6/30/2017

**VI. Roles and Responsibilities**

**A. Project Roles and Responsibilities**

**Agency Director:** Paul Matson

**Agency Deputy Director:** Anthony Guarino

**Agency Chief Information Officer (CIO):** Kent Smith

**Project Sponsor:** Kent Smith, CIO

**Project Manager:** Sandy Wang, Project Manager

**Technical Project Manager:** Molly Mahai, NIS Manager

**Firewalls Implementation Lead:** James Jarrel, Networking Analyst

**DLP Implementations Lead:** Tamera Wilson, Privacy Officer

**Multi-factor Authentication Implementation Lead:** John Davis, Networking Analyst

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

**B. Project Manager Certification**

- Project Management Professional (PMP) Certified
- State of Arizona Certified
- Project Management Certification not required

**C. Full-Time Employee (FTE) Project Hours**

<b>Total Full-Time Employee Hours</b>	1040
<b>Total Full-Time Employee Cost</b>	\$78,000

**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 <a href="http://aset.azdoa.gov/security/policies-standards-and-procedures">http://aset.azdoa.gov/security/policies-standards-and-procedures</a> , and applicable to this project? If <b>NO</b> , 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 <b>YES</b> , 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	\$223,705.92
Total Project Cost	VII. PIJ Financials tab	\$348,537.92
FTE Hours	VI. Roles and Responsibilities	1040

### C. Agency Approvals\*

Contact	Printed Name	Signature	Email and Phone
Project Manager:	Sandy Wang		
Agency Information Security Officer:	Gary Hummel		
Agency CIO:	Kent Smith		
Project Sponsor:	Anthony Guarino		
Agency Director:	Paul Matson		

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](mailto:ADOA-ASET_Webmaster@azdoa.gov)