ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title: Email Security Update - Attack Protection

Agency Name:	***Arizona Department of Health Services***
Date:	**9/8/2014**
Agency Contact Name:	**Raghu Ramaswamy**
Agency Contact Phone:	
Agency Contact Email:	

Hover for Instructions

I. Management Summary*

ADHS is updating its email security gateway appliance with new functionality and higher availability. The new functionality will prevent targeted email attacks (phishing emails). A second hardware appliance will provide the high availability and redundancy for the email gateway.

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:
6T

☐ **Yes** ☒ **No** Will a Request for Proposal (RFP) be issued as part of the Pre-PIJ or PIJ?

III. Business Case

*A. Business Problem**

Targeted email attacks containing malicious links and/or malicious email attachments represent one of the most dangerous IT threats facing enterprises today. According to the 2013 Verizon Data Breach Report, 95% of targeted attacks began with a spear-phishing attack, a single, carefully crafted email that tricked a recipient to click a link to install malware or surrender their login credentials. ADHS is very dependent on email and has been a target of a few phishing attacks so would like to implement additional protections. In addition, we have a Enterprise Security appliance that we would like to ensure is highly available so we are purchasing an additional appliance for redundancy.

*B. Proposed Business Solution**

has a product that offers email attack protection, Targeted Attack Protection. This product helps enterprises to add additional layers of security scrutiny. It takes an entirely new approach, using big data analysis techniques and a cloud architecture to identify suspicious email messages containing malicious URLs. Targeted Attack Protection represents the industry's first comprehensive email analysis solution for combating targeted threats using a full lifecycle approach, monitoring suspicious messages and email attachments as they come in, and observing user clicks as they attempt to reach out.

In addition, we are purchasing an additional appliance for redundancy of our Enterprise Security appliance (P660 Messaging Security Gateway). This secondary appliance would take over for the primary whenever the primary appliance is unavailable.

*C. Quantified Benefits**

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

Explain:

Service Enhancement—adding an additional Messaging Security Gateway appliance will offer high availability/redundancy. The appliances will be in an active/standby mode. The second appliance would take over for the primary whenever there is maintenance or an availability issue occurs. This proposed solution is not for a DR scenario.

Risk Avoidance--Spear-phishing attacks are a big risk. This product will help with the risk reduction of those particular threats. The secondary appliance will reduce the risk to availability of the email security gateway.

IV. Technology Approach

*A. Proposed Technology Solution**

ADHS proposes the purchase of the Targeted Attack protection for the Enterprise Email Security system. An additional Email Security Gateway appliance will be part of the proposed solution.

Appliance Scalability

Enterprise Email Security appliances offer high-performance, easy deployment and optimal scalability.

Enterprise Email Security appliances offer a convenient way to deploy the email security and compliance features of Enterprise Protection and Enterprise Privacy on premises.

Email Security appliances are designed to meet the unique anti-virus security needs of large enterprises, ISPs, universities, and government organizations. Email Security appliances offer all of the performance, flexibility, scalability, customization and end user control features needed in large-scale deployments. All security policy management and administration tasks are controlled via centralized, web-based administration console.

Each and every component of the email security system is engineered to meet the rigorous anti-virus security demands of enterprise performance. From the hardened, email messaging-optimized OS used in the email security

appliances, to the unique, queue-less architecture that allows all message scanning functions to be performed in memory, providing high performance.

’s email security appliances scale indefinitely to support many millions of email messages per day. Email security gateways can easily be deployed in multiple-appliance, master/agent configurations to support complex or geographically distributed data centers—offering the security of 100% redundancy combined with the convenience of a single administrative interface.

Targeted Attack Protection™ takes an entirely new approach, using Big Data analysis techniques and a Cloud Architecture to identify suspicious email messages containing malicious URLs or malicious email attachments. This helps enterprises to add additional layers of security scrutiny that cannot be matched by traditional security solutions and gateways. Targeted Attack Protection represents the industry's first comprehensive email analysis solution for combating targeted threats using a full lifecycle approach, monitoring suspicious messages and email attachments as they come in, and observing user clicks as they attempt to reach out. The key aspects of this email threat analysis solution include:

1) **Next-generation Detection:** Dynamic Malware Analysis Service enables detection of sophisticated targeted attacks, including those using polymorphic and zero-day malware, malicious attachments, and other advanced exploits.

   Benefit: Cloud scale and elasticity for malware analysis and sandboxing with global and immediate benefit to all organizations for emerging campaigns, with proprietary technology to defeat malware through counter-evasion techniques.

2) **Big Data driven prediction:** and real-time scoring engine utilizing a cloud-based statistical model to predict URL destinations likely to be malicious as part of an emerging attack.

   Benefit: Proactively identify threats and minimize clean-up for incident response teams by catching malicious URLs before users click and get infected.

3) **Follow-me Protection:** Unique URL re-writing of links within all suspicious emails to enable click-time protection via the URL Defense Service that is agnostic to browser, user device, and user location.

   Benefit: Enables security controls to persist, even if users are off the corporate network and bypassing on premise security controls.

4) **End-to-End Insight:** The Threat Insight Service provides a graphical dashboard and analysis report view for administrators and security professionals to obtain details of targeted attacks, identification of specific users that were attacked, and real-time notifications for potential incidents that require investigation.

Benefit: Know who clicked, when, and the threat forensics to enable rapid incident response and remediation.

B. Technology Environment

Email Security Gateway appliances – Intel based appliance with Intel Xeon 64bit Quad core CPU 8GB RAM, 300 GB Raid Storage will be part of the solution. The configuration of the new appliance will be done by the vendor. The high availability is accomplished through network connectivity like a firewall pair. This device acts like an email firewall.

C. Selection Process

is the existing vendor for our Enterprise Email gateway.

V. Project Approach

*A. Project Schedule**

Project Start Date: 9/15/2014 **Project End Date**: 11/3/2014

B. Project Milestones

Major Milestones	Start Date	Finish Date
Purchase equipment / services	9/15/014	9/22/2014
Enable Targeted Attack Protection (TAP) and URL defense / Configuration	9/22/2014	10/31/2014
Second appliance installed	10/1/2014	10/15/2014
Testing	10/16/2014	10/30/2014
Go Live		11/3/2014

VI. Roles and Responsibilities

A. Project Roles and Responsibilities

1.0 Project Sponsor Information Technology Executive – Paula Mattingly, Assistant Director / Chief Information Officer - This position will be accountable to place the necessary Information Technology at the Enterprise level and to meet the goals within the budget and timeline. Specific responsibilities will include (but not be limited to):

- Project champion, provides direction and support to ITS team
- Implement necessary Infrastructure and meet the immediate business needs
- Monitoring business value
- Management of IT staff or other resources
- and support to the team
- Sets the priority of the project

2.0 Information Security Project Manager – John Stark, Information Security Manager - This position will provide leadership and overall project management and efforts described in this document and for the future technology needs of the Department.

3.0 Project Security Support - Steve Newton - This position will provide technical analysis, software configuration, testing and deployment support.

- Coordinate implementation of appliance
- Implement and test policies for confidential information
-

4.0 Email Support Engineer – Calvin Hamilton This position will provide technical analysis, software configuration, testing and deployment support.

B. Project Manager Certification

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

C. Full-Time Employee (FTE) Project Hours

Total Full-Time Employee Hours	40
Total Full-Time Employee Cost	$ 1,800

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?	**Yes**	
2. Is this project referenced in your agency's Strategic IT Plan?	**Yes**	
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.	**Yes**	
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.		**No**
5. Is this project in compliance with the Arizona Revised Statutes (A.R.S.) and GRRC rules?	**Yes**	
6. Is this project in compliance with the statewide policy regarding the accessibility to equipment and information technology for citizens with disabilities?	**Yes**	

*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	**$0.0**
Total Development Cost	VII. PIJ Financials tab	**$35,038.17**
Total Project Cost	VII. PIJ Financials tab	**$139,023.50**
FTE Hours 40	VI. Roles and Responsibilities	**$1,800**

*C. Agency Approvals**

Contact	Printed Name	Signature	Email and Phone
Project Manager:	Steve Newton		
Agency Information Security Manager:	John Stark		
Agency CIO: **Project Sponsor:**	Paula Mattingly		
Agency CFO:	Jim Humble		
Deputy Director of Planning and Operations:	Janet Mullen		
Agency Director:	Will Humble		

IX. Optional Attachments

A. Vendor Quotes

Glossary

X. Additional Information

Links:

ADOA-ASET Website

ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:

Strategic Oversight

ADOA-ASET_Webmaster@azdoa.gov