ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title:

AHCCCS Security Enhancement 2014 PIJ

Agency Name:	**AHCCCS**
Date:	**April 25, 2014**
Agency Contact Name:	**Joanne Obenour**
Agency Contact Phone:	
Agency Contact Email:	

Hover for Instructions

I. Management Summary*

AHCCCS proposes to improve the security plan and enhance its risk management by adding penetration testing tools and to remediate the security risk identified by improving its secure email product.

The penetration test tool will allow us to run simple penetration tests on our web applications prior to implementation as well as prior to major upgrades. This would be in addition to regular periodic external third-party penetration tests/audits. The purpose of the penetration testing is to proactively identify potential security risks with our web applications. The proposed product is the Pro Version of Rapid7 Metasploit.

As part of our security plan, we need to improve our existing secure email product, Global Certs Secure Mail Gateway. This was a recommendation/finding in our latest security audit. We propose to replace it with Symantec Messaging Gateway Content Encryption. The functionality allows us to send email in a secure (encrypted) fashion.

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:
Click here to enter text.

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

III. Business Case

*A. Business Problem**

AHCCCS is continuously and proactively improving the security posture of the Agency. We have two business issues discussed in this PIJ: they are penetration testing and secure email.

Penetration testing is currently performed by contracting with a third party to provide us with independent assessments. We want to be more proactive and also enhance this process by running internal (by AHCCCS) penetration tests, while continuing our external assessments. This would allow us to identify and remediate any identified issues as we implement major web application upgrades.

Our existing secure email product is not as secure as we would like it to be. This was a finding in our security assessment. We need to replace it with a more secure product. AHCCCS uses secure mail when sending emails containing PHI/sensitive data.

*B. Proposed Business Solution**

For penetration test tool, AHCCCS proposes to implement the Pro Version of Rapid7 Metasploit product. The product is secure and allows for a simple implementation. The product will be managed and utilized by a team of staff at AHCCCS including our network, web applications, and security teams. Limited training will be provided. The use of this product will be to provide simple penetration tests of AHCCCS' web applications. This includes the Hawaii web applications as well. Penetration testing tools range from simple to very complex as well as their associated price tags. We chose this product because it meets our basic needs and from recommendations we received.

The secure email product proposed will allow us to securely send emails containing PHI/sensitive information. It is a Symantec product which will easily integrate with their product suite that we already have running in the AHCCCS environment.

*C. Quantified Benefits**

- [ ] Service enhancement
- [ ] Increased revenue
- [ ] Cost reduction
- [ ] Problem avoidance
- [x] Risk avoidance

Explain:

Minimizing security risk is a top priority of the Agency, especially with the volume of the PHI and PII data handled on a daily basis. Our approach is to continuously conduct self-audits and tests along with regular external third party audits, and to remediate critical findings.

IV. Technology Approach

*A. Proposed Technology Solution**

Replace the existing secure email (Global Certs Secure Mail Gateway) with an encrypted solution (Symantec Messaging Gateway Content Encryption) that is SOC3/SysTrust certified (this certification ensures that a company operation uses best practices in the areas of security, integrity, availability, and confidentiality as well as demonstrates their effectiveness over a period of time).

Implement the penetration testing tool, Pro version of Rapid7 Metasploit.

B. Technology Environment

The new secure email product, Symantec Messaging Gateway Content Encryption, will be operated on existing AHCCCS infrastructure (facility provided by ADOA Data Center) while the data (secure email content) will be in a secured environment.

The penetration test tool will be operated on existing AHCCCS infrastructure by AHCCCS staff. It will help improve AHCCCS' security posture by proactively identifying and

remediating security vulnerabilities found via penetration testing. This would be in addition to external third party assessments.

C. Selection Process

Approach was to remediate critical audit findings in a prioritized manner according to the availability of funding and resources. We incorporated third party assessment findings and suggestions into our selection of the penetration tools. Any new hardware or software purchases would be compatible to the existing network infrastructure. The proposed secured email replacement is compatible with our existing infrastructure because we already operate Symantec's Suite of products.

V. Project Approach

*A. Project Schedule**

Project Start Date: 4/1/2014 **Project End Date**: 9/30/2014

B. Project Milestones

Major Milestones	Start Date	Finish Date
Acquisition	4/1/2014	5/1/2014
Installation for Testing	5/1/2014	6/1/2014
Component Testing	5/1/2014	6/1/2014
System Testing	5/1/2014	6/1/2014
Implementation	6/1/2014	6/30/2014
Post Implementation Support	7/1/2014	9/30/2014

VI. Roles and Responsibilities

A. Project Roles and Responsibilities

The Data Security Team along with Network Services will work together to test and implement these products.

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	1000
Total Full-Time Employee Cost	$50,000

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 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	**$50,795**
Total Project Cost	VII. PIJ Financials tab	**$61,532**
FTE Hours	VI. Roles and Responsibilities	**1000**

C. *Agency Approvals**

Contact	Printed Name	Signature	Email and Phone
Project Manager:			
Agency Information Security Officer:	Jim Wang		
Agency CIO:	Jim Wang		
Project Sponsor:	Jim Wang		
Agency Director:	Tom Betlach		

IX. Optional Attachments

A. Vendor Quotes

X. Glossary

XI. Additional Information

AHCCCS uses role-based security so that participants can only access what they need to perform their job functions.

Links:

ADOA-ASET Website

ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:

Strategic Oversight

ADOA-ASET_Webmaster@azdoa.gov