ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification
(PIJ)

A Statewide Standard
Document for Information Technology Projects

Project Title: ***Network Security FY2014***

Agency Name: ***Arizona Department of Revenue***
Date: ***Oct. 7, 2013***
Prepared By: ***Conrad DeLaCruz, Monique Gregory***

Revised PIJ Version – January 2013

TABLE OF CONTENTS

ASET Forms:

Project forms are available on the ADOA ASET website – see links below

Project Investment Justification Documents - http://aset.azdoa.gov/content/project-investment-justification

Project Oversight Status Report and Change Request Form – http://aset.azdoa.gov/sites/default/files/media/docs/StatusRpt%26ProjChangeForm_0.xls

Web Development Initiatives - Notice of Intent (NOI) form – http://aset.azdoa.gov/node/15

I. General Information {A}

I.A General Information {A}

Agency CIO:	Carole Martin	**Contact Phone:**	
Agency Contact Name:	Monique Gregory	**Contact Phone:**	
Agency Contact Email:		**Prepared Date:**	Oct. 7, 2013

I.B Special Funding Considerations {A}

☐ **Yes** ☒**No - Does this project require funding approved for a Pre PIJ Assessment phase?**

II. Project Overview

II.A Management Summary {A}

This project expands the Department of Revenue's information protection mechanisms. Specifically encryption technologies and improve our network security posture. DOR has received funding for the FY2014 Budget year to support this project.

1. Encryption – deploy encryption technologies to further protect confidential information acquired from citizens and businesses for data which is stored (at rest) and data which is transmitted (in transit).
2. Network Upgrades – implement additional network hardware and software to protect the network infrastructure with current network technology, and to manage and mitigate threats when they occur.
3. Encryption Engineers – to provide technical encryption expertise and analyses in implementing the agency encryption posture

I. Problem Description

Safeguarding systems and protecting data is never a completed task. Proactive and continual update and replacement of security tools is required in order to ensure data is safeguarded and the network remains resilient and available to support agency-critical applications and a workforce that depends on availability of services and information.

Per Executive Order 2008-10, (reference found here http://azgovernor.gov/dms/upload/EO%202008-10_v2.pdf) the State must endeavor to protect confidential information it acquires from its citizens and businesses through the deployment of encryption technologies. Encryption technologies protect confidential information using algorithms and key mechanisms. DOR's protection mechanisms for confidential information include encryption. This project expands the encryption capability.

To provide a reliable, performance-based service to the Agency and its stakeholders in this technology-centric environment, DOR has designed and configured a LAN/WAN network with no single points of failure. To ensure this network is resilient and available to support agency-critical applications and a workforce that depends on availability of services and information, it is

important to secure and protect the network against attack from inside and out and ultimately provide proactive analysis and response tools to manage attacks.

II. Solution

In collaboration with the ADOA-ASET, ADOR will implement several security enhancements to improve the Department of Revenue's security profile. These enhancements include:

- Data Center Network planning, design, and implementation services
  - Enhanced mass storage encryption
  - Enhanced database encryption
  - Enhanced full disk encryption
  - Enhanced backup and archive media encryption

- Network Software and Hardware for Data Center

  - Upgrade intrusion detection and prevention at DOR, its data centers and the disaster recovery site.

- Staffing Augmentation costs – Software and Storage qualified engineers

III. Quantified Justification

Performance Measures to quantify the success of the solution:

The measurement for the DOR Risk Management approach in dealing with continuing malicious attacks will be validated by the following actions:

- Use of strong encryption with a well-known and community-tested encryption algorithm.
- Strong key management technology and processes.
- Role-based access controls in conjunction with encryption and key management implementation.
- Testing and Auditing to ensure data is properly encrypted and that there are no issues with the deployment.
- Stronger encryption improves DOR's ability to repel malicious attacks
- Routine audits of operational systems to ensure that policies are being followed and the system is working properly.

II.B Existing Situation and Problem, "As Is" {A}

The personally identifiable information collected by the Department in the course of executing its duties is a continuous target of malicious attacks. Currently DOR experiences a Denial of Service attack via SPAM at its mail security appliance every night with attempts to harvest the contacts in the email directory. Overall government websites are the number one attack target on the Internet.

Information protection requires a broad spectrum of technologies to detect and prevent data compromise; many technologies successfully thwart daily attempts to compromise our network. Funds from this request will increase our ability to protect taxpayer information

In response to the state-wide need to protect confidential information, the Arizona Statewide Information Security and Privacy Office (SISPO), under the direction of Arizona Strategic Enterprise Technology Office, a division of the Arizona Department of Administration, created the Statewide Information Security Standard P800-S850 Encryption Technologies.

"PURPOSE This standard establishes acceptable criteria for the use of encryption technologies for securing confidential data/information to mitigate information risks for the State of Arizona. As a custodian of public and confidential information, the state must further protect private and sensitive data/information from all cyber threats and vulnerabilities whether external or internal to the state. "

- Excerpted from Arizona Statewide Information Security Standard P800-S850

  It is the duty of the Department of Revenue ("Department") to ensure the protection taxpayer information from unauthorized disclosure. The appropriate mechanism, encryption, is identified by the SISPO standard.

This State Standard is further supported by Information Security Best Practices for the protection of confidential information includes encryption of information. (National Institute of Standards and Technology, U.S. Dept. of Commerce Pub 800-53; the International Organization for Standardization, ISO 27001; the Federal Information Processing Standards, FIPS 140-2).

The threat of information theft from government agencies is very real:

- Last year, the S.C. Department of Revenue announced that 3.8 million Social Security numbers, 3.3 million bank account numbers and information from almost 700,000 businesses had been exposed to cyber-attack. This breach resulted in costs of approximately $20.1 million to the State of South Carolina. (references found here: http://www.bankinfosecurity.com/20-million-loan-to-cover-breach-costs-a-5355 and http://www.thestate.com/2013/01/06/2578924/the-latest-on-sc-hacking-costs.html

II.C Proposed Changes and Objectives, "To Be"

In collaboration with the ADOA-ASET Information Secuirty group, DOR will implement several security enhancements to enhance the DOR Risk Management approach in dealing with continuing malicious attacks and reduce the amount of security risk across the enterprise.

II.D Proposed Technology Approach {Required for Pre-PIJ Assessment Only}

Not Applicable

III. Project Approach

III.A Proposed Technology

Implementation of enhanced encryption of all Department data will be in a phased approach. Encryption is not a single technology. It includes network hardware to protect data from threats, software to encrypt data at servers, software to encrypt data on disks, software to encrypt data while it traverses the network within and between buildings and a 'key' system to manage rights to 'lock' and 'unlock' the information. Encrypted data is larger than its unencrypted counterpart, by 8% on average, increasing disk capacity requirements. Servers have to unencrypt data to perform application functions, and then re-encrypt the data to move or store it, increasing server capacity requirements to prevent significant degradation of end-user response time. The National Institute of Standards and Technology identifies several hardware and software technologies for consideration when encrypting.

During FY14, we will:

> Implement available hardware, software and services for the ADOR network and ADOR disk infrastructure that will proactively augment threat protection solutions and enhance the existing ADOR network while further protecting Arizona state tax payer information and state information systems.

III.B Other Alternatives Considered

Option 1- Do Nothing – maintaining the network security as it is today limits DOR's ability to protect its systems against future risks. As a result, DOR data could be compromised due to an undetected malicious activity. **Determination:** This could result in system downtime, data compromise, and loss of revenue from IRS data in collections activity (currently $33 million per year) and extra costs to provide credit monitoring services to constituents.

Alternatives considered and reasons for rejection:

Option 2- Outsourcing network security to DOA. **Determination**: Current ADOA Shared services are not fully matured in these technology areas. While it is a DOR IT Strategic goal to migrate to ADOA Centers of Excellence for non-agency specific services, ADOA is still developing these capabilities. Throughout this initiative we will invest in inter-agency collaboration, with the goal of maximizing the opportunity to use ADOA services to manage assets procured through this investment.

III.C Major Deliverables and Outcomes

Major Deliverables and outcomes of the project are as follows:

- Enhanced mass storage encryption
- Enhanced database encryption
- Enhanced full disk encryption
- Enhanced backup and archive media encryption

IV. Policies, Standards & Procedures

IV.A Enterprise Architecture

☒ **Yes** ☐**No -** Does this project meet all 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 as applicable for this project?

If **NO** please describe ***NEW*** or ***EXCEPTIONS*** to Standards {Network, Security, Platform, Software/Application and/or Data/Information}:

IV.B Service Oriented Architecture Planning and Implementation

☐ **Yes** ☒**No -** Does this project qualify as an SOA application by improving application delivery for technology reuse and /or application reuse and / or services reuse?

IV.C Disaster Recovery Plan and Business Continuity Plan

☒ **Yes** ☐**No -** Does this project require a Disaster Recovery Plan and Business Continuity Plan?

IV.D Project Operations

☐ **Yes** ☒**No -** Is there a written assessment of short-term and long-term effects the project will have on operations?

IV.E Web Development Initiative

☐ **Yes** ☒**No -** Is this a Web Development initiative? If **YES**, a Notice of Intent (**NOI**) must be provided. Link: http://aset.azdoa.gov/node/15

IV.F IT State Goals

Please check which goal the project is in support of; if more than one, indicate only the primary goal.

- ☐ Accelerate Statewide Enterprise Architecture Adoption
- ☐ Champion Governance, Transparency and Communication
- ☐ Invest in Core Enterprise Capabilities
- ☒ Proactively Manage Enterprise Risk
- ☐ Implement a Continuous Improvement Culture
- ☐ Adopt Innovative Sustainability Models
- ☐ Reduce Total Cost of Ownership
- ☐ Improve Quality, Capacity and Velocity of Business Services
- ☐ Strengthen Statewide Program and Project Management
- ☐ Build Innovative and Engaged Teams
- ☐ Other_____

V. Roles and Responsibilities

V.A Project Roles & Responsibilities:

Please identify Project Roles & Responsibilities:

Network and Information Security staff in conjunction with appropriate vendor information security engineering resources will be responsible for configuring, deploying, and managing the enhanced security infrastructure.

The agency PMO will oversee and direct this project.

The Agency Information Security Officer will participate in the planning and implementation of this project.

Please indicate Project Manager Certification:

The **project manager** assigned to the project is:
- ☐ Project Management Professional (PMP) Certified
- ☒ State of Arizona Certified
- ☐ PM Certification not required

VI. Project Benefits

VI.A Benefits to the State

***Score:* 0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive.**

Description	*Score*
Agency Performance: The extent to which duties and processes will improve or positively affect business functions. Consider reduced redundancy and improved consistency for the agency.	2
Productivity Increase: The improvements in quantity or timeliness of services or deliverables. Consider improved turnaround time or expanded capacity of key processes.	1
Operational Efficiency: Efficiencies based on improved use of resources, greater flexibility in agency responses to stakeholder requests, reduction or elimination of paperwork, legacy systems, or manual tasks.	1
Accomplishment Probability: The extent to which this project is expected to have a high level of success in completing all requirements for the division or agency.	5
Functional Integration: The impact the project will have in eliminating redundancy or improve consistency. Consider the impact of information sharing between departments, divisions, or agencies in the State.	2
Technology Sensitive: The implementation of the right types of technology to meet clear and defined goals and to support key functions. Consider technologies and systems already proven within the agency, division, or other similar organizations.	5
Total	16
Additional Information *(provide details on Benefits that score > 3)*	
Describe additional details on benefits > 3 score. Also provide details on any savings that may be applicable.	

VI.B Value to the Public

***Score:* 0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive.**

Description	*Score*
Client Satisfaction: Rate how stakeholders may respond to anticipated improvements. This could apply to health and welfare services, quality of life or life safety functions.	4
Customer Service: Rate anticipated improvements to internal and external customer service delivery. Give consideration to faster response, greater access to information, elimination or reduction in client complaints.	1
Life Safety Functions: Applies to public protection, health, environment, and safety. Consider how this project will reduce risk in these functions.	2
Public Service Functions: Applies to licensing, maintenance, payments, and tax. Consider how this project will enhance services in these functions.	0
Legal Requirements: Consideration should be given to projects mandated by federal or state law. Other consideration could be given if there are interfaces with other federal, state, or local entities.	5
Total	12
Additional Information *(provide details on Value to the Public scores > 3)*	
Describe additional details on scores > 3.	
As a custodian of public and confidential information, the primary value to the public is risk mitigation and further protection of private and sensitive data/information from all cyber threats and vulnerabilities whether external or internal to the state.	

VII. Project Timeline {A}

VII.A Project Schedule

Provide <u>estimated</u> schedule for the development of this project. These dates are estimates only; more detailed dates will be required at project start up once the project schedule is established.

Project Start Date:	**August 2013**	**Project End Date:**	**November 2014**

NOTE – Project spend will be completed by the end of FY14 as required

VIII. Project Financials

Project Funding Details **Select One**

☐ **Pre PIJ Assessment Funding Details Only**
☒ **Full PIJ Project Funding Details**

VIII.A Pre-Assessment Project Financials {Required for Pre-Assessment PIJ Only}

Not Applicable

VIII.B Detailed Project Financials {Required for PIJ Approval}

Development and Operational Project Funding Details

Funding Categories:

Professional and Outside Services: *The dollars to be expended for all third-party consultants and contractors.*
Hardware: *All costs related to computer hardware and peripheral purchases for the project.*
Software: *All costs related to applications and systems related software purchases for the project.*
Communications: *All costs related to telecommunications equipment, i.e. switches, routers, leased lines, etc.*
Facilities: *All costs related to improvements or expansions of existing facilities required to support this project.*
License & Maintenance Fees: *All licensing and maintenance fees that might apply to hardware, software and any other products as up-front costs to the project (ongoing costs would be included under Operational expense).*
Other: *Other IT costs not included above, such as travel, training, documentation, etc.*
NOTE*: FTE costs may be included in section VIII.e below, as required.*

VIII.C Funding Source {A}

(Double click on table below – add funding in **whole dollars** and then click outside the table to return to Word doc)

Funding Source Category	Name of Funding Source	Currently Available ($)		New Request ($)		Total ($)
		Development Budget	Operational Budget	Development Budget)	Operational Budget	
General Fund				$ -		$ -
Federal ARRA Fund						$ -
Federal Fund						$ -
Other Appropriated Funds	Automation Fund	$ 4,900,000	$ 1,796,000	$ -		$ 6,696,000
Other Non Appropriated Funds						$ -
TOTAL PROJECT COSTS (Should = development and operational totals above)		$ 4,900,000	$ 1,796,000	$ -	$ -	$ 6,696,000

VIII.D Special Terms and Conditions (if required) {A}

Special Terms and Conditions (if required)

VIII.E Full Time Employee Project (FTE) Hours

Provide estimated FTE Development hours that will be utilized for the duration of the project. Include IT as well as Business Unit FTE hours, if available. Enter into Project Values table on Approvals page. **Enter FTE costs (if known) as well.**

Total Full Time Employee Hours	5,800
Total Full Time Employee Cost (loaded)	$321,900
Supplemental services from ADOA-ASET Information Security group	**$ 0**

IX. Project Classification and Risk Assessment

IX.A Project Classification and Risk Assessment Matrix

Rate each question to determine risk level at Low (0), Medium (1), High (2), Very High (3).

Enter Risk Score into Project Values table on Approvals page.

RISK EVALUATION RANGES

LOW RISK PROJECT	0 - 8
MEDIUM RISK PROJECT	9 - 25
HIGH RISK PROJECT	26 - 42
VERY HIGH RISK PROJECT	43 +

Add Project Risk Details (if required)

PIJ Project Classification & Risk Evaluation					
Risk Factor	**Low (0)**	**Medium (1)**	**High (2)**	**Very High (3)**	**Score**
Project Management Complexity					
Project Team Size (# of people)	1-5	6-10	11-15	> 15	2
Project Manager (PM) Experience	Deep experience in this type of project	Some experience in this type of project and able to leverage subject matter experts	Some experience in this type of project and has limited support from subject matter experts	New to this type of project	1
Team Member Availability	Dedicated staff for project activities only as assigned	Staff is in place, few interrupts for non project tasks are expected and have been accounted for	Available, some turnover expected, some interrupts for non project issues likely	Dedicated team not available; staff will be assigned based on capacity	2
# of Agencies involved in Development activity	1	2	3	> 3	0
Vendor (if used)	No Vendor required	Vendor has been used previously with success	Vendor has been used previously with some management support required	New Vendor and/or multiple vendors	1
Project Schedule	Schedule is flexible	Schedule can handle minor variations, but deadlines are somewhat firm	Scope or budget can handle minor variations, but deadlines are firm	Scope, Budget and Deadlines are fixed and cannot be changed	2
Project Scope	Scope is defined and approved	Scope is defined and pending approval	Scope being defined	High level definition only at this point	1
Budget Constraints	Funds allocated	Funds pending approval	Allocation of funds in doubt or subject to change without notice	No funding allocated	0
Project Methodology	Defined methodology	Defined methodology, no templates	High level methodology framework only	No formal methodology	0
IT Solution Complexity					
Product Maturity (if purchased)	Product implemented & working in > 1 state agency or business of similar size	Product implemented & working in 1 agency or business of similar size	Product implemented & working only in an agency or business of smaller size	Product not implemented in any agency or business	1
Solution Dependencies	No dependencies or interrelated projects	Some minor dependencies or interrelated projects but considered low risk	Some major dependencies or interrelated projects but considered medium risk	Major high-risk dependencies or interrelated projects	0
System Interface Profile	No other system interfaces	1-2 required interfaces	3-4 required interfaces	> 4 required interfaces	0
IT Architectural Impact	Follows State IT approved design; principles, practice & standards	New to the State but follows established industry standards	Evolving "industry standard"	No standards, leading edge technology	0
Deployment Impact					
Process Impact	No business process changes	Agency wide process changes	Multi-State Agency process changes	State-wide process changes	0
Scope of End User Impact	Department or Division level only	Multiple Division or Agency wide impacts	Multi-Agency impacts	State-wide impacts	1
Training Impact	No training is required	Minimal training is required	Considerable training is required	Extensive training is required	1
				Total Risk Score	**12**

X. Project Approvals

X.A CIO Review {A}

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 consistent with agency and State policies, standards and procedures?	X	
4. Is this project in compliance with the Arizona Revised Statutes and GRRC rules?	X	
5. Is this project in compliance with the statewide policy regarding the Accessibility to Equipment and Information Technology for Citizens with Disabilities?	X	
6. Is this project mandated by law, court case or rule? If yes, cite the federal requirement, ARS Reference or Court Case. Details: Arizona Revised Statue (ARS) Title 42 Chapter 2 Article 1 defines taxpayer and taxpayer transactional information as "Confidential". It further proh bits the disclosure of confidential information. A. R. S. § 42-1001.6 directs the Department of Revenue ("Department") "Provide information and advice within the scope of its duties subject to the laws on confidentiality of information and departmental rules adopted pursuant to laws." 42-001.7 requires the Department "Advise with and make recommendations to the governor and legislature on all matters concerning its objectives. " The personally identifiable information collected by the Department in the course of executing its duties is a continuous target of malicious attacks. Information protection requires a broad spectrum of technologies to detect and prevent data loss; many technologies successfully thwart daily attempts to compromise our network. In response to the state-wide need to protect confidential information, the Arizona Statewide Information Security and Privacy Office (SISPO), under the direction of Arizona Strategic Enterprise Technology Office, a division of the Arizona Department of Administration, created the Statewide Information Security Standard P800-S850 Encryption Technologies. "PURPOSE This standard establishes acceptable criteria for the use of encryption technologies for securing confidential data/information to mitigate information risks for the State of Arizona. As a custodian of public and confidential information, the state must further protect private and sensitive data/information from all cyber threats and vulnerabilities whether external or internal to the state. " "STANDARD Encryption technologies protect confidential information during transmission over state networks and in storage by using algorithms and a key mechanism which renders information unreadable for unauthorized intruders on state systems. The information is mathematically protected against disclosure and cannot be read by someone who does not have a corresponding key to decrypt the information. Encryption is a defense-in-depth strategy for the protection of informational assets of the state. Therefore, all Budget Units shall deploy the use of encryption and protection techniques as listed below for the transmission of confidential data/information over state networks and as final repository in technology storage devices. " - Excerpted from Arizona Statewide Information Security Standard P800-S850 It is the duty of the Department of Revenue ("Department") to ensure the protection taxpayer information from unauthorized disclosure. The appropriate mechanism, encryption, is identified by the SISPO standard.	X	

X.B Project Values

Description	Section	Significance
Assessment Cost *{A}*	VIII. Project Financials **{Required for Pre-Assessment PIJ Approval Only}**	$
Economic Benefits	VI. Benefits to the State	16
Value Rating	VI. Value to the Public	12
Total Development Cost	VIII. Project Financials	$4,900,000
Total Project Cost	VIII. Project Financials	$6,696,000
FTE Hours	VIII. Project Financials	
Project Risk Factors	IX. Risk Summary	12

X.c Project Approvals {A}

Select One ☐ **Pre PIJ Assessment Approval Only** ☒ **PIJ Project Approval**

Project Title:

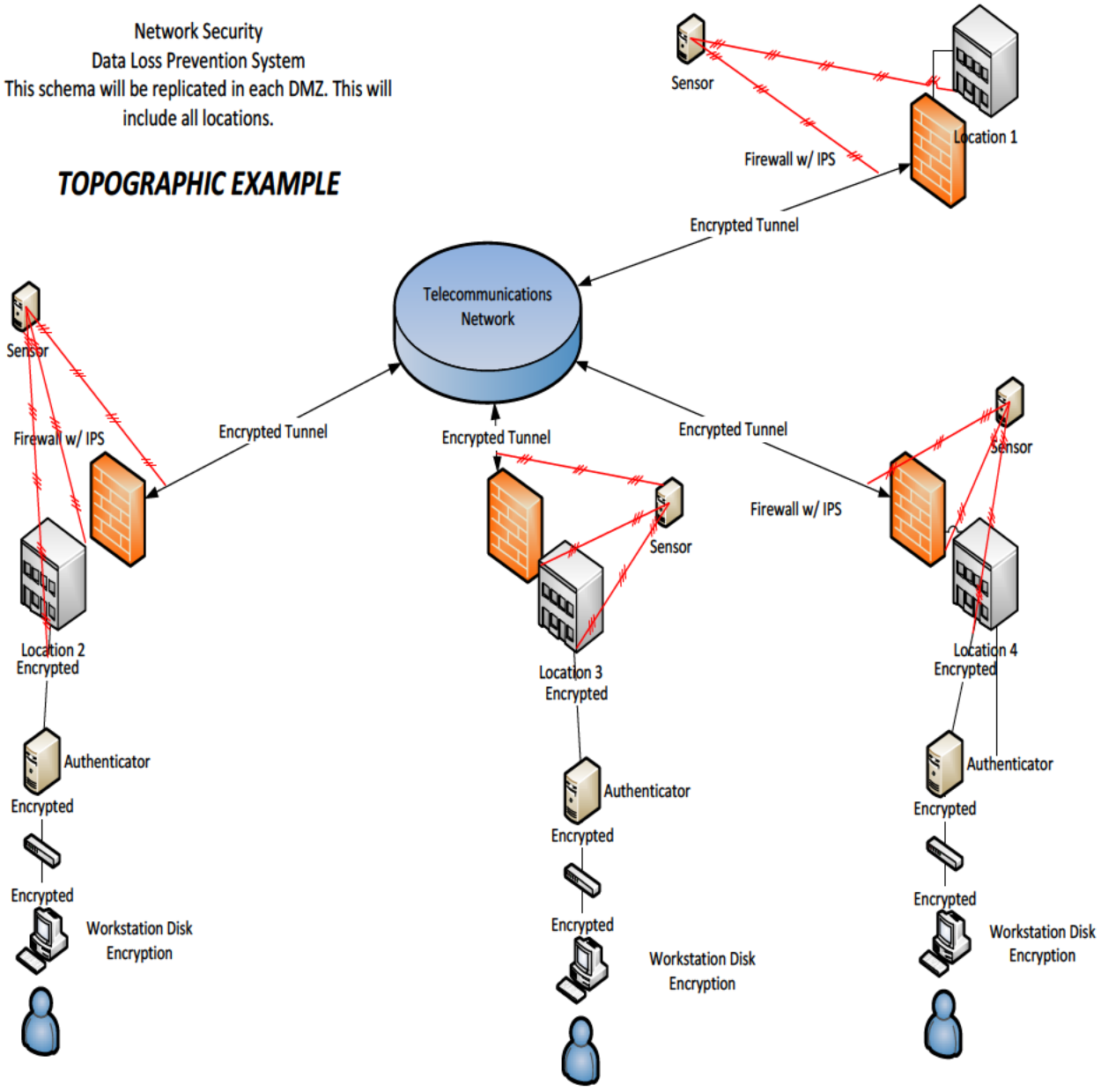
Responsibility	*Printed Name*	*Approval Signature*	*Date*
Project Manager:	Monique Gregory		
Agency CIO:	Carole Martin		
Acting Agency CISO	Fawn Medesha		
Acting Agency Director:	David Raber		

Appendix

A. Itemized List with Costs

Pre- Quote provided

B. Connectivity Diagram



C. Project Schedule - Gantt Chart or Project Management Timeline

Intrusion Detection and Prevention can be completed within 60 days after receipt of equipment.

Upgrades to remote office perimeter and endpoint security requires onsite work and will be scheduled with consideration of other Network Services projects.

Encryption upgrades will be implemented and rolled out in a phased implementation.

Milestone	Begin Date	End Date
ASET Review and Approval	**August 2013**	**September 2013**
JLBC Review and Approval	**August 2013**	**October 2013**
Intrusion Prevention System & Network switches	**September 2013**	**February 2014**
Procure Hardware and Software	September 2013	November 2013
Install Hardware and Software*	October 2013	February 2014
Upgrade Office Perimeter & Endpoint Security	**November 2013**	**June 2014**
Procure Hardware and Software	November 2012	December 2013
Install Hardware and Software*	January 2014	June 2014
Encryption Upgrade	**November 2013**	**November 2014**
Procure Hardware and Software	December 2013	February 2014
Install Hardware and Software*	February 2014	October 2014
Project Closeout		November 2014

*Installation includes required training

D. NOI (Web Projects Only)

Not Applicable

Glossary

Document Information

Title: Project Investment Justification – PIJ Version January 2013
Originator: Arizona Department of Administration – AZ Strategic Enterprise Technology Office
Date: January 2013
Download: http://aset.azdoa.gov/
Contacts: **ASET Oversight Managers:**
http://aset.azdoa.gov/content/project-investment-justification

Web Design (NOI Contact):
http://aset.azdoa.gov/webtools