ADOA – ASET
Arizona Strategic Enterprise Technology

Project Investment Justification
(PIJ)

A Statewide Standard
Document for Information Technology Projects

Project Title: ***Arizona State Hospital Wireless Network***

Agency Name: ***Arizona Department of Health Services***
Date: ***7/1/13***
Prepared By: ***Janet Slawinski***

Revised PIJ Version – January 2013

Contents

PROJECT INVESTMENT JUSTIFICATION (PIJ) TEMPLATE DECISION MATRIX

After determining the category of project, complete the sections of the PIJ or PIJ Lite document as indicated below. All projects with $25,000 or more in development expense require that a PIJ or PIJ Lite be approved by ASET. All projects with $1,000,000 or more in development expense require a PIJ to be approved by the Information Technology Authorization Committee (ITAC) as well.

ASET may request additional information or require completion of additional sections, if the project is deemed critical in nature.

Category	PIJ Lite	Pre PIJ *	PIJ	ITAC Review
Low Risk projects: Including Operational Infrastructure Upgrades *(i.e. PC Replacement/Refresh, Network Upgrades)*	●			
Medium Risk projects		Optional	●	
High Risk projects		Optional	●	
Very High Risk projects		Optional	●	
$1.0M and Above projects		Optional	●	●

Section	Category	PIJ Lite	Pre PIJ *	PIJ	Add for ITAC $1.0M+
I.	**General Information**				
I.A	**General Information**	●	●	●	
I.B	**Special Funding Considerations**		●	●	
II.	**Project Overview**				
II.A	**Management Summary**	●	●	●	
II.B	**Existing Situation & Problem, "As Is"**	●	●	●	
II.C	**Proposed Changes & Objectives, "To Be"**	●	●	●	
II.D	**Proposed Technology Approach**		●		
III.	**Project Approach**				
III.A	**Proposed Technology**	●		●	
III.B	**Other Alternatives Considered**			●	
III.C	**Major Deliverables & Outcomes**	●		●	
IV.	**Policies, Standards & Procedures**				
IV.A	**Enterprise Architecture**	●		●	
IV.B	**Service Oriented Architecture Planning & Implementation**			●	
IV.C	**Disaster Recovery Plan & Business Continuity Plan**			●	
IV.D	**Project Operations**			●	
IV.E	**Web Development Initiative**			●	
IV.F	**IT State Goals**			●	
V.	**Roles and Responsibilities**				
V.A	**Roles and Responsibilities**	●		●	
VI.	**Project Benefits**				
VI.A	**Benefits to the State**			●	
VI.B	**Value to the Public**			●	
VII.	**Project Timeline**				
VII.A	**Project Schedule**	●	●	●	
VIII.	**Project Financials**				

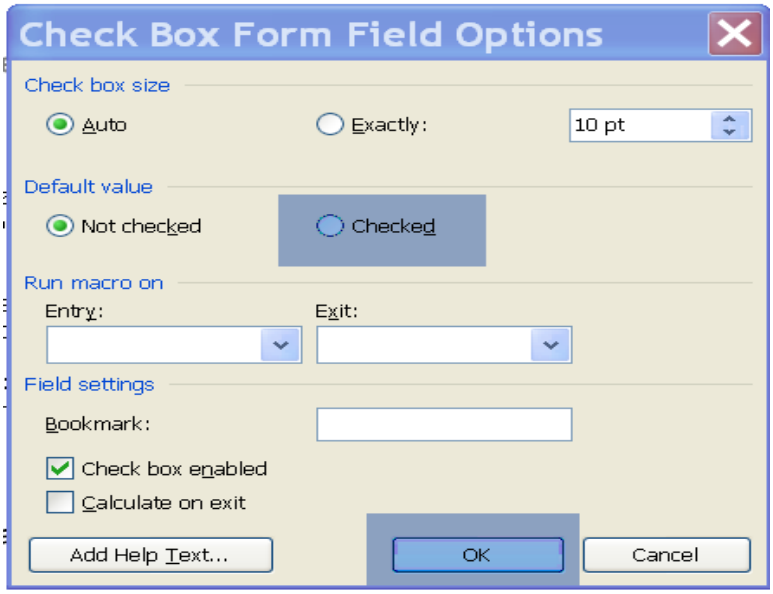
VIII.A	**Pre-Assessment Project Financials**		●		
VIII.B	**Detailed Project Financials**	●		●	
VIII.C	**Funding Source**	●	●	●	
VIII.D	**Special Terms and Conditions (if required)**	●	●	●	
VIII.E	**Full Time Employee (FTE) Hours**	●		●	
IX.	**Project Classification & Risk Assessment**				
IX.A	**Project Classification & Risk Assessment Matrix**	●		●	
X.	**Project Approvals**				
X.A	**CIO Review**	●	●	●	
X.B	**Project Values**	●	●	●	
X.C	**Project Approvals**	●	●	●	
Appendix					
A	**Itemized List with Costs**	●		●	
B	**Connectivity Diagram**				●
C	**Gantt Chart, Project Management Summary**				●
D	**NOI (Web Projects Only)**	●		●	

* **Pre PIJ** is optional for agencies seeking approval from external entities to contract for outside labor or resources to assess scope, technology and approach. After the assessment is completed, full project details will be added to the PIJ for final PIJ Approval.

NOTE: ***Pre PIJ Assessments are not required for all projects but up to the discretion of the Agency.***

Document Instructions:

Double click on square ☐ **Yes** ☐**No** and select “checked” for the appropriate box then select “OK”.



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

I.A General Information

Agency CIO:	Paula Mattingly	**Contact Phone:**	
Agency Contact Name:	Raghu Ramaswamy	**Contact Phone:**	
Agency Contact Email:		**Prepared Date:**	7/1/13

I.B Special Funding Considerations

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

If **YES**, provide details for the **Pre PIJ Assessment** funding needs by filling out the areas marked with **{A}** or **{Required for Pre-PIJ Assessment only}**. Further information and details will be required after the assessment for the Final PIJ approval.

If **NO**, provide details for the Final PIJ by filling out **all** areas **excluding** those sections marked with **{Required for Pre-PIJ Assessment only}**.

II. Project Overview

II.A Management Summary

The Arizona State Hospital (originally deeded as the Insane Asylum of Arizona in 1885 by the 13th Territorial Legislature) opened for business in 1887 on the 93 acre campus located at 24th Street and Van Buren in Phoenix to treat the most severely mentally ill residents in the state. In 1998, as a result of legislation, the State Hospital opened the Arizona Community Protection and Treatment Center (ACPTC), which provides treatment services to sexual offenders who are deemed to be a threat to the community. Campus facilities include treatment units for approximately 300 civil and forensic patients and 100 residents of the ACPTC program. Approximately 700 employees work at the State Hospital, which operates 24 hours a day 7 days a week.

The State Hospital's automated system of record is the electronic medical record (EMR), which contains patient demographic data, as well as clinical assessments and treatment information. Medical and clinical providers such as doctors, nurses, rehabilitation staff, dietitians, therapists and many other staff members need to routinely make entries or update information in the EMR.

I. Problem Description

Due to the size of the campus, clinicians spend much of their time traveling from one building to another in order to provide treatment services to patients. Although there are currently approximately 400 desktop computers in use at the hospital, an inadequate number are deployed on the treatment units due to limitations of physical space and infrastructure. In addition, some areas of the treatment units that are accessible to patients, such as group treatment rooms, are intentionally not equipped with network drops or computers due to safety and infection control concerns. Where space is an issue, computers are shared by staff, particularly during the day shift when staffing levels are the highest, meaning that staff members frequently need to wait for a computer to become available in order to make entries into the EMR. This causes delays in entering clinical updates and progress notes, or may cause errors since staff are relying on hand written notes that must be keyed in at a later date and time. These delays prevent the information

from being shared with other treatment team members as quickly and efficiently as possible. In addition, timeframes for completing clinical documentation are dictated by various accrediting bodies, including the Joint Commission (TJC) and Centers for Medicare and Medicaid Services (CMS). A lack of timely and accurate documentation in the EMR can result in audit exceptions, revocation of the hospital license, financial sanctions and potentially have a negative impact on patient outcomes.

The EMR system is used to provide reports and information that assist medical personnel in delivering treatment to patients at the hospital. In addition, the system produces required reports for the legislature, the Governor's Office of Strategic Planning and Budget, and the Joint Legislative Budget Committee. All personnel must have adequate access to the EMR to ensure that all patient documentation is accurate, complete, up-to-date, and available for sharing across disciplines and with external partners.

In FY 2008 and 2009, wireless capabilities were successfully implemented at the State Hospital but due to funding limitations, coverage was extended only to the Civil side of the campus, providing coverage in only four of approximately thirty buildings (see map in Appendix B).

II. Solution

The proposed solution is to install a Wireless Local Area Network (WLAN) throughout the hospital campus, which would allow the use of laptops, tablets, and other mobile devices to enter clinical information and other patient data into the EMR from anywhere on the campus, without the need for a hard-wired device. The mobile devices and wireless infrastructure will ensure adequate system access and provide staff members the ability to make entries directly into the system, eliminating the need to create a hard copy of their work. Medical and clinical personnel depend on the EMR system to obtain and document critical treatment information including medications, clinical treatment notes, and test results. Expanded access to the EMR through the use of mobile devices will result in improved patient care.

World Wide Technology (WWT) Professional Services performed a WLAN Site Survey for the Arizona State Hospital. The goal of the analysis was to determine the proper placement of access points to provide a pervasive wireless infrastructure capable of supporting data wireless capabilities. The result of this analysis is a document which provides the Arizona State Hospital a detailed report that shows where wireless access points are required to support the future wireless network requirements (see Appendix C, Connectivity Diagram).

ADHS proposes to procure and implement the WWT solution of two hundred and ten (210) access points to be connected over new Category 5e cabling to LAN switches providing Power over Ethernet (PoE). This includes replacing the 40 access points currently located on the Civil side of the campus. Two wireless LAN controllers will also be purchased and configured. ADHS has selected Cisco's Identity Services Engine (ISE) as the software solution for ensuring the integrity and security of the end user devices (up to 250 devices for the initial implementation). The ISE solution will replace the existing Access Control Server used to secure the State Hospital's wireless network. WWT will install the access points and additional cabling, provide services to implement the ISE in conjunction with Information Technology Services (ITS) network staff, and conduct a post-implementation site survey to ensure that coverage is as expected.

III. Quantified Justification

Wireless Local Area Networks allow workers to access and contribute information far more quickly than before, boosting the productivity of all workers who depend on that critical information and, hence, increasing the overall agility of the agency. Up-to-date patient information will be entered and shared more timely, which will improve patient care. The hospital will be assured of meeting the timeliness requirements of governing authorities. WWT successfully implemented the existing wireless network at the State Hospital and has considerable experience implementing wireless capabilities in other health care facilities.

II.B Existing Situation and Problem, "As Is"

Currently, there is not enough physical space on the hospital's treatment units to provide a one-to-one ratio of desktop computers to staff, nor is the technical infrastructure sufficient to expand access. Adding computers would require extensive wiring and additional power, which would be costly and extremely

disruptive to staff and patients. In addition, some areas on the treatment units were intentionally left unwired and computer-free due to patient safety concerns. Many of the group treatment planning and therapy sessions take place in these rooms, requiring either the dictation of notes for later transcription and entry into the EMR, or reliance on handwritten notes, which also need to be entered into the EMR at a later time. The existing wireless capabilities provide coverage in only four out of approximately thirty buildings.

World Wide Technology Professional Services performed a WLAN Site Survey for the Arizona State Hospital. The goal of the analysis was to determine the proper placement of access points to provide a pervasive wireless infrastructure capable of supporting data wireless capabilities. The result of this analysis is a document which provides the Arizona State Hospital a detailed report that shows where wireless access points are required to support future wireless network requirements. The purpose of the Wireless Site Survey was to:

- Plan for a new deployment of wireless coverage at several Arizona State Hospital office locations.
- Identify possible sources of interference.
- Identify sub-optimal access point installation locations and make recommendations for relocation of access points when required.

An active site survey was performed using AirMagnet Survey Pro. Coverage areas that did not meet the requirements of Arizona State Hospital were described, along with recommendations to remediate the wireless coverage in these areas. As determined by the analysis performed under the design restrictions detailed above, two hundred and ten (210) Access Points (APs) will be required.

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

ADHS proposes procuring and implementing the WWT proposed solution of two hundred and ten (210) APs to be connected over new Category 5e cabling to LAN switches providing Power over Ethernet (PoE). The WWT solution will provide the necessary coverage, capacity, client roaming and data throughput required to support the data applications defined for use on the wireless network. The wireless network will expand access to the EMR through the use of mobile devices in areas that are not currently set up with hard-wired equipment and will eliminate the need for staff to wait for shared computers to become available. This will improve daily operational efficiency and patient care.

Wireless technology offers opportunities for substantially improving healthcare processes and providing a unified communication framework for staff members. Technology advances include:

- Strengthened communication security, in support of patient privacy regulations.
- Push data delivery, ensuring prompt notification in the event of medical crises or urgent situations.
- Dual-mode connectivity (combining cellular and Wi-Fi), minimizing barriers to communication inside buildings or while traveling on the campus.
- Single point of contact through integrated applications, providing better coordination of communication tasks among doctors, nurses and support staff members.
- Improved access to vital electronic medical records (EMR), decision support tools, medical references and similar resources.

Wireless Security

Security needs to be paramount and a major consideration for any WLAN deployment. The inherently open nature of wireless access – compared to the wired world – creates significant security concerns, especially user authentication and data encryption. Broadcast signals often travel into public areas that can be accessed by eavesdropping individuals who have not passed through any type of authentication process to validate their presence at the site. The site survey should identify the security status of all locations considered for wireless access. To secure the Arizona State Hospital campus wireless network, ADHS will implement security policies and mechanisms that keep outsiders out and insiders honest. Fully protecting the WLAN means:

- Preventing external hackers from getting access to the network
- Allowing only authorized users into the network
- Preventing those inside the network from executing deliberate or inadvertent attacks

- Monitoring of the network to identify rogue WLANs, detect intruders and impending threats, and enforce WLAN security policies.

To be truly effective, the security policy must accomplish these goals in a way that is transparent to the users, easy to administer, and does not disrupt business. The following section describes the security model that will be used to secure the State Hospital's wireless network.

III. Project Approach

III.A Proposed Technology

One of the key factors in determining the success of a WLAN deployment is a site survey. A great deal of information can be obtained from the site survey, but even more important is how that information is analyzed to support cell planning; cell search threshold; range and throughput; interference/delay spread; bandwidth management for applications like voice over WLAN; access point density, and load balancing.

Technical Specifications:

World Wide Technology performed a wireless site survey at the State Hospital to specify the location of access points to provide signal coverage and data throughput for the wireless infrastructure. The WWT proposed solution will require two hundred and ten (210) APs connected over new Category 5e cabling to LAN switches providing Power over Ethernet (PoE). The Access Points will be managed by two Cisco Series 5700 WLAN controllers. ADHS will secure the end user devices using Cisco's Identity Services Engine. Professional services from WWT will be procured for the installation of the wireless network, additional Category 5 cabling, and the ISE implementation. Ongoing management of the network will be the responsibility of ADHS technical staff.

Infrastructure Security Model

Below is the ADHS Infrastructure Security Model to be maintained for the proposed wireless access points, including authentication and use of WPA2 enterprise protocols.

- Authentication, Authorization, and Accounting (AAA) – AAA provides a coherent framework to represent and define the ADHS wireless network security design.
- Authentication refers to the process of obtaining and validating the user's identity. ADHS will use robust encrypted authentication techniques by leveraging WPA2 / PEAPv0 / MSCHAPv2. PEAP is a secure choice for Microsoft Active Directory and Apple mobile device configurations.
- Authorization provides access control based upon the identity of each person attempting to authenticate to the DHS wireless network. A rich set of enforcements and conditional restrictions are utilized.
- Accounting provides detailed information for auditing and reporting end-user sessions.
- Access Control Measures.
- IEEE 802.1x framework.
- Access Control List (ACL).
- Network Security Control Measures.
- VLAN membership.
- Physical security control measures.

Enhanced Protection Measures

- ADHS will enable per-user authentication (restricted to authorized employees and/or contractors)
- ADHS will enable per-session encryption
- ADHS will enable RADIUS
- ADHS will enable virus-scanning software on client devices
- ADHS will configure Firewalls to control access the wireless resources
- ADHS will enable RFC 1918 and RFC 2827 for inbound traffic
- ADHS will install FIPS 140-2 tamper evidence seals (installed on each Access Point)
- ADHS will configure Network Boundary of Control

- ADHS will disable Guest access
- ADHS will disable the SSID broadcast feature
- ADHS will disable Bluetooth access
- ADHS will enforce wireless authentication
- ADHS will enforce wireless authorization
- ADHS will enforce wireless confidentiality
- ADHS will ensure wireless endpoint integrity checking
- ADHS will ensure Non-repudiation.

Endpoint Integrity Checking

ADHS will ensure client devices meet the defined security profile before the client device is allowed a connection to the ADHS wireless network. ADHS has selected the Cisco Identity Services Engine (ISE) for this purpose. For comprehensive device security, ISE ensures a seamless integration with market leading Mobile Device Management (MDM) platforms to ensure enhanced device security and policy compliance. The Cisco ISE is an all-in-one enterprise policy control product that enables comprehensive secure wired, wireless, and VPN access, leading to more productive workers and lower operational costs. Key features include rigorous identity enforcement, extensive policy enforcement, security compliance, automated onboarding, automated device security, dependable anywhere access, operational efficiency, embedded enforcement, and next-generation policy enforcement.

Compliance Model

ADHS will adhere to:

- FIPS 140-2
- HIPAA
- NIST
- Statewide Standard P800-S820, Authentication and Directory Services
- Statewide Standard, P800-S830 Rev 3.0 Network Security
- Statewide Standard, P800-S850 Encryption Technologies.

HITRUST Common Security Framework (CSF)

The ADHS framework will be comprised of HITRUST's CSF. The HITRUST CSF contains 13 security control categories comprised of 42 control objectives and 135 control specifications which map to HIPAA Security rule and other compliance requirements.

Operational Readiness:

The ADHS is well-positioned to implement and support the proposed technology and has experienced technical resources capable of supporting the new infrastructure as described below.

Permitted Devices

ADHS already owns over 100 tablets, 300 smartphones, and 700 laptops. Each device using Microsoft Windows is encrypted with McAfee Endpoint Protection, or in the case of the agency's Apple devices, PASSCODE encryption is enforced via the Mobile Device Management (MDM) system-AirWatch. McAfee Endpoint protection enables pre-boot authentication.

- Agency Approved Device Types
    - Laptops
    - Smartphones
    - Tablets

Information Security Controls

Below is a list of security controls currently utilized by the agency:

- Cisco Firewalls -- with botnet filtering
- Cisco Iron Port S650 Web Proxy, AV
- RSA Envision -- SEIM
- Cisco IPS 4255 (IDS)

- Trustwave Network Monitor (DLP) - Vericept
- Cisco Identity Services Engine (ISE) – ADHS is considering this solution.

Monitoring Capabilities

ADHS Audit & Special Investigations and the Information Security Office will monitor the wireless infrastructure per below:

- ADHS will conduct random security audits (performed in-house)
- ADHS will conduct annual security audits and vulnerability scanning
- ADHS will conduct real-time Internet monitoring
- ADHS will maintain an Intrusion Detection and Prevention System (IDPS).

Risk Management Methodology

The ADHS Information Security program performs regular risk assessments and risk management. Assessments are conducted annually as required by State Wide Policy (P800 Standard S805 Rev 2.0 – IT Risk Management) for information technology (IT) systems and their environments to determine security vulnerabilities.

Ongoing Operations

- Configuration Management
  - ADHS will conduct routine maintenance to ensure the wireless network is at or near the proposed vendor patch level.
- Lifecycle Management
  - ADHS developed a system life-cycle document to forecast the wireless network refresh schedule.
- Network Administration is conducted by 1 FTE Network Engineer and 1 FTE LAN Admin.
- Information\network security is performed by 1 FTE Information Security Manager and 1 FTE Network Security Manager.

III.B Other Alternatives Considered

The other option considered was purchasing additional desktop computers and placing them in each unit. This was not seen as a viable option as it would require extensive additional wiring in units, the purchase of additional computers, and would take up additional space within the units where space is already limited. In addition, there are areas within the treatment units where network drops and desktops are not advisable due to patient safety concerns.

III.C Major Deliverables and Outcomes

Deliverables:

- Purchase wireless infrastructure – ADHS
- Install/configure wireless infrastructure – WWT
- Deploy wireless infrastructure – WWT, ADHS
- ISE Implementation – WWT, ADHS
- Post-Implementation Site Survey – WWT, ADHS

Outcomes: As a result of this project, medical personnel and other clinicians will have expanded access to the EMR, enabling up-to-date medical records that will immediately be available to all personnel who need this information for patient care and regulatory purposes.

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:

1.0 Project Sponsor – Donna Noriega – This position will provide approval for project scope. Specific responsibilities will include (but not be limited to):

- Project champion, provides direction and support to the team
- Approves project scope and funding and sets the priority.

2.0 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.

3.0 Information Technology Project Manager – Janet Slawinski, ITS Project 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.

4.0 Network Engineer – Eric Hill -- This position will provide technical analysis, configuration, testing and deployment support.

5.0 Receiving – This position will tag the equipment prior to installation and configuration.

6.0 Professional Services - WWT -- Provides design, build, installation, configuration, and testing.

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.	5
Productivity Increase: The improvements in quantity or timeliness of services or deliverables. Consider improved turnaround time or expanded capacity of key processes.	5
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.	5
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.	5
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	30

Additional Information *(provide details on Benefits that score > 3)*

Agency Performance: *Implementing a wireless infrastructure will mobilize the state hospital workforce as they perform daily EMR system updates and modify patient data via a mobile device.*

Productivity Increase: *The wireless infrastructure will increase the productivity of the state hospital workforce by enabling EMR system updates as staff traverses the campus.*

Operational Efficiency: *The wireless infrastructure will benefit the agencies primary information system users by providing access to the EMR system.*

Accomplishment Probability: *The probability of accomplishment is high considering the success the agency has had with previous wireless implementation.*

Functional Integration: *Implementing a wireless infrastructure to deliver business critical services will ensure the success of service delivery and avoid a possible loss of productivity and possibly death.*

Technology Sensitive: *The technology selected by the agency has a proven track record across the United States.*

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.	5
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.	5
Life Safety Functions: Applies to public protection, health, environment, and safety. Consider how this project will reduce risk in these functions.	5
Public Service Functions: Applies to licensing, maintenance, payments, and tax. Consider how this project will enhance services in these functions.	5
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	25

Additional Information *(provide details on Value to the Public scores > 3)*

Client Satisfaction: *Stakeholders will be pleased at the agencies efficiencies gained by implementing the wireless infrastructure.*

Customer Service: *Patient care will improve by enabling more robust access to patient data.*

Life Safety Functions: *The project will improve access to patient data, thus improving direct patient care.*

Public Service Functions*: The wireless infrastructure will improve access to the EMR system and other hospital applications*

Legal Requirements: *ADHS is required to provide these services as mandated by state law.*

VII. Project Timeline {A}

VII.A Project Schedule

Provide estimated 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: **Project End Date:**

Note: Installation of this wireless network is dependent upon AzNet completing the switch replacement project first. Once that is scheduled, the wireless implementation will be scheduled with WWT. The estimated completion for this project is 3 – 6 months after PIJ approval.

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}

Project Funding Details for Pre-Assessment Project Investment Justification Only

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

ESTIMATED COSTS						
Category	*FY____*	*FY____*	*FY____*	*FY____*	*FY____*	*Total*
Assessment Costs						$ -
Development Costs						$ -
Total Development Costs (including Assessment)	$ -	$ -	$ -	$ -	$ -	$ -
Operational Costs (if estimate is available)						$ -
Total Estimated Project Costs	$ -	$ -	$ -	$ -	$ -	$ -

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	HPP Grant	$ 510,626	$ 33,190			$ 543,816
Other Appropriated Funds						$ -
Other Non Appropriated Funds	ASH Fund		$ 96,048			$ 96,048
TOTAL PROJECT COSTS (Should = development and operational totals above)		$ 510,626	$ 129,238	$ -	$ -	$ 639,864

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

Special Terms and Conditions (if required)
Hardware, software, and partial maintenance costs are being funded out of Hospital Preparedness Program (HPP) grant funds which must be expended by August 31, 2013. Breakdown of how these funds will be expended is as follows: Hardware: $ 256,234 Software: $ 17,288 Maint. FY 2014 $ 1,174 Maint. FY 2015 $ 32,016 Total $ 306,712

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	160
Total Full Time Employee Cost	$5,484

Note: FTE hours are for the Network Engineer who will work with WWT on the ISE configuration.

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	0
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	0
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	0
# 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	1
Project Scope	Scope is defined and approved	Scope is defined and pending approval	Scope being defined	High level definition only at this point	0
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	0
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	1
System Interface Profile	No other system interfaces	1-2 required interfaces	3-4 required interfaces	> 4 required interfaces	1
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	1
Scope of End User Impact	Department or Division level only	Multiple Division or Agency wide impacts	Multi-Agency impacts	State-wide impacts	0
Training Impact	No training is required	Minimal training is required	Considerable training is required	Extensive training is required	1
				Total Risk Score	**6**

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: *Provide details related to technology as part of the requirement.*		X

X.B Project Values

The following table contains summary information taken from the other sections of the PIJ document.

Description	Section	Significance
Assessment Cost *{A}*	VIII. Project Financials **{Required for Pre-Assessment PIJ Approval Only}**	$
Economic Benefits	VI. Benefits to the State	30
Value Rating	VI. Value to the Public	25
Total Development Cost	VIII. Project Financials	$510,626
Total Project Cost	VIII. Project Financials	$639,864
FTE Hours	VIII. Project Financials	160
Project Risk Factors	IX. Risk Summary	6

The PIJ must be transmitted to ASET by email as a Word document. Project approvals may be sent to ASET by email in PDF format. Include the Project Title below for identification. Send to your ASET Oversight Manager, or if not sure who is assigned to your Agency, PIJ docs can be sent to ASET_Projects@azdoa.gov.

X.c Project Approvals {A}

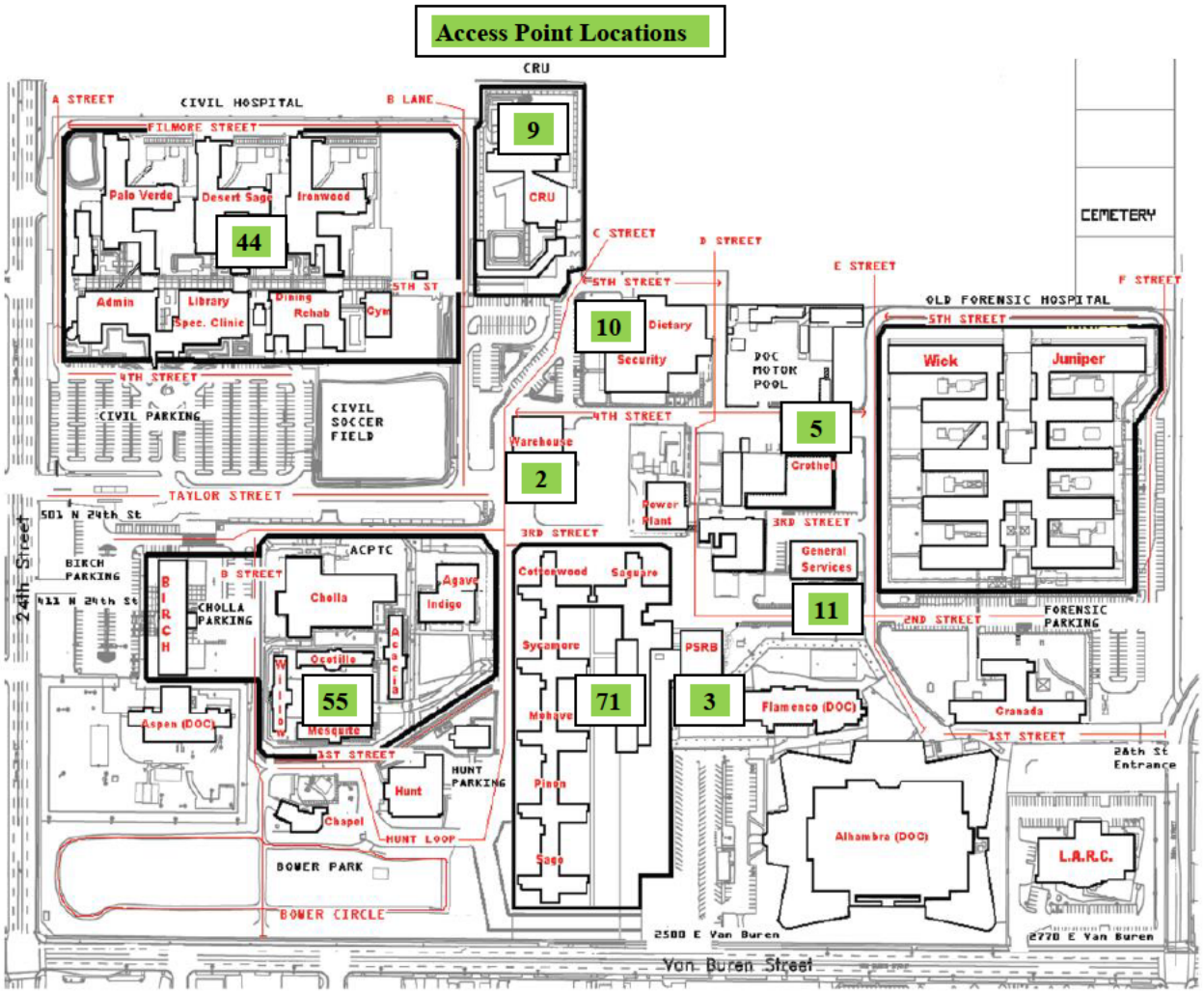
Select One ☐ **Pre PIJ Assessment Approval Only** ☒ **PIJ Project Approval**

Project Title: Arizona State Hospital Wireless Upgrade

Responsibility	*Printed Name*	*Approval Signature*	*Date*
Project Manager:	Janet Slawinski		
Agency CIO:	Paula Mattingly		
Project Sponsor:	Donna Noriega		
Deputy Director:	Cory Nelson		
CFO:	Jim Humble		
Deputy Director:	Janet Mullen		
Agency Director:	Will Humble		

Appendix

B. Connectivity Diagram (ASH Campus Map)



C. Project Schedule - Gantt Chart or Project Management Timeline

NOTE: Scheduling is dependent upon AzNet scheduling and completing the switch replacement project.

D. NOI (Web Projects Only)

Not applicable to this project.

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