ADOA-ASET

Arizona Strategic Enterprise Technology

Project Investment Justification

Version 01.01

A Statewide Standard Document for Information Technology Projects

Project Title:

AZDPS CI/KR Database

Agency Name:	**Arizona Department of Public Safety**
Date:	**June 6, 2014**
Agency Contact Name:	**Stephen M. Harrison**
Agency Contact Phone:	
Agency Contact Email:	

Hover for Instructions

I. Management Summary*

The Department of Public Safety is mandated through state statute ARS §41-1803, *to establish and operate a statewide critical infrastructure information system*. The Intelligence Bureau, through the Arizona Counter Terrorism Information Center (ACTIC) currently utilizes the Department of Homeland Security's (DHS), Automated Critical Asset Management System (ACAMS) to meet this mandate. The Intelligence Bureau learned on June 4, 2014, DHS will decommission the ACAMS system effective Friday, June 6, 2014; therefore, the Intelligence Bureau is in need of pursuing the ability to establish and operate a statewide critical infrastructure information system. The ACAMS system will be replaced by another system; Infrastructure Protection Gateway (IP Gateway). ACAMS and IP Gateway each have significant deficiencies for state use. Neither system allows access for facility manager's to input or update their own information. First responder's are unable to access the system. IP Gateway is designed to collect comprehensive data about critical infrastructure. IP Gateway does not allow the state to collect information about Key Resources, such as k-12 schools. The Intelligence Bureau wishes to acquire the appropriate software and hardware to establish and operate a statewide critical infrastructure information system

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**

The Department of Public Safety is mandated through state statute ARS §41-1803, *to establish and operate a statewide critical infrastructure information system*. The Intelligence Bureau currently utilizes the Department of Homeland Security's (DHS), Automated Critical Asset Management System (ACAMS) to meet this mandate. The Intelligence Bureau has learned DHS will no longer support the ACAMS system effective sometime in 2014; therefore, the Intelligence Bureau is in need of pursuing the ability to establish and operate a statewide critical infrastructure information system.

*B. Proposed Business Solution**

There are no off the shelf Critical Infrastructure/Key Resource database systems available. Working with a current vendor, nFocus (formerly General Dynamics) we have identified a solution of developing a state system, which will be web based and allow access for facility managers to enter and update their own Critical Infrastructure

information. nFocus working with DPS input will develop a solution that is capable of meeting the needs of Public Safety in Arizona. The proposed solution is to use nFocus' existing system, TraxSolutions and integrate that system with the current DPS owned Geosuite system for accessibility by first responders. Additionally, Public Safety personnel, with the appropriate system security and permissions will be able to access Critical Infrastructure/Key Resources information. The ACTIC has been in communication with DHS and there is a plan to transfer the existing ACAMS data into the new Arizona System.

*C. Quantified Benefits**

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

Explain:

Currently the state does not have its own Critical Infrastructure/Key Resources database that is accessible to facility managers or Public Safety personnel responding to one of these facilities. ARS §41-1803 mandates the Department of Public Safety *establish and operate a statewide critical infrastructure information system.* The proposed solution would provide for that system. The system, as proposed, would provide access to detail facility information for Public Safety personnel responding to an emergency at one of the facilities, potentially mitigating loss of life, injuries or property damage. Additionally, as part of the facility manager's questionnaire, appropriately trained Public Safety personnel would provide feedback to facility manager's to better secure their facility, potentially mitigating risks to their facility.

IV. Technology Approach

*A. Proposed Technology Solution**

The proposed Technology Solution is outlined in the Statement of Work, as well as, the End User License Agreement. The Critical Infrastructure/Key Resources database will be an enhancement to the department's current system, GeoSuite. GeoSuite is a web-based, multimedia common operation system that allows users to collect report and share information. Geosuite was acquired by DPS in 2013. It improves situational awareness and facilitates collaboration and information sharing and analysis between users.

The Critical Infrastructure/Key Resources solution will consist of a Hosted Service, which includes a TraxSolutions server and an additional GeoSuite Core Server, located in a secure Hosted Data Center in Phoenix. Geosuite and nFocus products are currently purchased through the state contract with SHI. As Asset and Facility Managers in the State commit to contributing their Critical Infrastructure/Key Resources information, they will be able to answer a set of questions on the TraxSolutions web-facing server. By answering these questions and uploading supporting artifacts regarding the Critical

Infrastructure/Key Resources, the corresponding information will be available to the Terrorism Liaison Officers to make a site visit and assessment. Following the Facility assessment, the information will be uploaded into GeoSuite. The non-PCII information will be posted to the First Responder GeoSuite system already in operation at the department.

The configuration will consist of 1 TraxSolutions Server, 1 GeoSuite Core Server License for 100 Terrorism Liaison Officers, 1 TraxSolutions/GeoSuite Software Integration, and annual maintenance/support. Initially, the ACTIC will provide for administration of the Geosuite and CI/KR systems and provide for necessary access for vetted users. There is discussion of using Active Directory in future applications of the system; however, initially ACTIC personnel will manage account access and tracking users. The ACTIC will add and/or delete access as appropriate.

The network will meet the security standards for receiving, storing and transmitting Personally Identifiable Information. All data is transferred using 128-bit encryption Secure Sockets Layer (SSL). See attached nFocus documents for additional information related to physical security and application security. Beyond what is in Appendix the vendor has agreed to move the hosted service to the Amazon AWS GovCloud US, which is FedRamp compliant.

B. Technology Environment

There currently is no DPS Critical Infrastructure/Key Resources information system. This proposed solution will fulfill the requirements of ARS §41-1803. The proposed vendor, nFocus, a subsidiary of General Dynamics, has the ability and authorization to store and transmit Personally Identifiable Information and its TraxSolutions system currently handles Protected Health Information

C. Selection Process

Other Fusion Centers and law enforcement agencies, as well as, web based search engines were utilized in an attempt to identify any Critical Infrastructure/Key Resources information systems currently in use or available Commercially Off the Shelf solutions. There were no Commercially Off the Shelf solutions identified. Some Fusion Centers and law enforcement agencies utilize Microsoft Excel or Microsoft Access and have created their own system to store Critical Infrastructure/Key Resources information. None of these solutions are available to Facility Managers to enter or update their own information, nor is the information available to first responders when responding to an emergency at one of these facilities. We have not discovered a system, currently available, that provides the capabilities the proposed solution will provide.

V. Project Approach

*A. Project Schedule**

Project Start Date: 6/9/2014 **Project End Date**: 12/31/2014

B. Project Milestones

Major Milestones	Start Date	Finish Date
Setup, installation and test of all component hardware and software for the Critical Infrastructure/Key Resources system	June 2014	July 2014
Integration of nFocus TraxSolutions server and GeoSuite Common Operating System. Deliver and Display date in near real-time from TraxSolutions to GeoSuite servers at AZDPS and in the Critical Infrastructure/Key Resources Hosted servers, visible to users state-wide	July 2014	December 2014
Provide continuous hosted service of the Critical Infrastructure/Key Resources solution, inclusive of maintenance, support and upgrades as appropriate	July 2014	June 2019

VI. Roles and Responsibilities

A. Project Roles and Responsibilities

The project will be overseen by the Arizona Counter Terrorism Information Center/Intelligence Bureau within the Criminal Investigations Division of the Department of Public Safety.

The project manager will be; Captain Stephen M. Harrison

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	160
Total Full-Time Employee Cost	$0

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	**$747500**
Total Project Cost	VII. PIJ Financials tab	**$747500**
FTE Hours	VI. Roles and Responsibilities	

C. *Agency Approvals**

Contact	Printed Name	Signature	Email and Phone
Project Manager:	Stephen M. Harrison		
Agency Information Security Officer:	Roger Baune		
Agency CIO:	Gregg Hayes		
Project Sponsor:	Major Mike Orose		
Agency Director:	Robert C. Halliday		

IX. Optional Attachments

A. Vendor Quotes

B. Statement of Work

C. End User License Agreement

D. nFocus Security Overview As of 21 May 2014

E. nFocus TraxSolutions; Data Security FAQ

X. Glossary

XI. Additional Information

See attachment D and E for additional information related to the security of PII information.

Links:

ADOA-ASET Website

ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:

Strategic Oversight

ADOA-ASET_Webmaster@azdoa.gov