ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Arizona State Retirement System (ASRS)

Information Protection and Security

RT19002

Arizona State Retirement System

Contents

1. GENERAL INFORMATION

PIJ ID: RT19002
PIJ Name: Arizona State Retirement System (ASRS) Information Protection and Security
Account: Arizona State Retirement System
Business Unit Requesting: Technology Services Division
Sponsor: Anthony Guarino
Sponsor Title: Deputy Director
Sponsor Email: anthonyg@azasrs.gov
Sponsor Phone: (602) 240-2077

2. MEETING PRE-WORK

2.1 What is the operational issue or business need that the Agency is trying to solve? (i.e....current process is manual, which increases resource time/costs to the State/Agency, and leads to errors…):

The primary goal of this project is to increase our security and reduce the risk of personally identifiable information (PII) data loss.

Our agency's "Clifton Larson Allen Privacy Assessment" gave low markings in the maturity area of "Use, Retention and Disposal" based on the Generally Accepted Privacy Principles (GAPP). The information security assessment performed by RiskSense in May 2017 was first focused on ASRS IT infrastructure and secondarily on ASRS developed applications. As a result, the findings did not always include information about ASRS applications even though the risk the control is designed to mitigate applies to ASRS developed applications as well. From the May 2017 RiskSense Information Security Assessment, the ASRS was rated as having a maturity rating less than 3 (of 5) for 7 of the NIST controls.

The results of these assessments have shown key areas where we can improve. There are several locations within our internal systems where we are displaying sensitive Personally Identifiable Information (PII) to an unnecessarily large internal user base. This information includes Social Security Number (SSN) and bank account numbers. We plan to address each of these problems individually using various strategies. Additionally, our internal systems need their logging standards increased so that we have more granular data about precisely who is doing what and when. If a security incident occurs we must be capable of providing the authorities with precisely who had access to a specific account or piece of data along with when it was accessed, what was viewed and who viewed it.

Glossary
ANI- Automatic Number Identification aka Caller ID
ANI Verification- The process/service that 3rd party vendors offer that attempts to validate the authenticity of the ANI data associated with a phone call.
ASET- Arizona Strategic Enterprise Technology
ASRS- Arizona State Retirement System
AZNET- The ADOA chosen vendor for the state phone system and call center system. It is managed by Century Link.
FileNet- Software solution used by ASRS for document, image and workflow management.
ID - Identification
IPS- Information Protection and Security, the name of this project at ASRS
ITAC- Information Technology Authorization Committee

IVR- Integrated Voice Response, the ASRS call center tool used to answer incoming calls and route callers.
GAPP- Generally Accepted Privacy Principles
NIST- National Institute of Standards and Technology
PERIS – Public Employees Retirement Information System, the original ASRS developed application to manage the information of members and beneficiaries and employers of the ASRS.
PID- Person ID, a unique number that ASRS uses in its database to uniquely identify a person record.
PII- Personally Identifiable Information, for this project the PII in question is SSN and bank account number.
PIJ- Project Investment Justification
POL- PERIS Online, the name of the internally developed ASRS application to manage the information of members and beneficiaries and employers of the ASRS.
SSN- Social Security Number, classified as Personally Identifiable Information

2.2 How will solving this issue or addressing this need benefit the State or the Agency?

Fixing these issues will reduce the risk of sensitive data being used for improper purposes and it will allow investigators to help identify who the potential culprits were. If PII is lost or misused it can have a huge impact on our members which will in turn create a large cost to the agency. If our data is misused the audit logging created by this project will give us the ability to identify potential culprits.

Benefits:

-Reduced access to PII along with Access logging, lowers our risk of internal fraud

-Securing member PII by eliminating SSN as the main identifier in multiple software systems

-Logging solution will provide valuable forensic data in the case of a breach

-Improved compliance with GAPP (Generally Accepted Privacy Principles)

2.3 Describe the proposed solution to this business need.

Phase 1: Modify FileNet to use PID

ASRS will transition to identifying people using “Person ID” (PID) for all internal purposes. This is an ASRS specific number that will meet our needs to identify people within the ASRS for all internal business purposes.

Phase 2: Replace PII within Applications

Systems/Screens that display SSN/bank account number will be modified to display a portion of the SSN/bank account number. Full SSN access can be granted to specific groups and all access will be logged.

Phase 3: Create new FileNet Document Class

A new FileNet document class will be created and utilized to store documents that might contain SSN or bank account number and additional security will be placed on this document class.

Phase 4: Data Access Logs

ASRS will add additional access logging for all ASRS applications. This will enable us to track exactly which user id has accessed any screen at the ASRS. We will create a reporting interface to provide useful access logs.

Phase 5: Call Center Changes- Eliminate prompting callers for SSN when calling into our call center. We propose using the caller’s Caller ID (ANI- Automatic Number Identification) data to attempt pre identification.

2.4 Has the existing technology environment, into which the proposed solution will be implemented, been documented?

Yes

2.4a Please describe the existing technology environment into which the proposed solution will be implemented.

2.5 Have the business requirements been gathered, along with any technology requirements that have been identified?

Yes

2.5a Please explain below why the requirements are not available.

3. PRE-PIJ/ASSESSMENT

3.1 Are you submitting this as a Pre-PIJ in order to issue a Request for Proposal (RFP) to evaluate options and select a solution that meets the project requirements?

No

3.1a Is the final Statement of Work (SOW) for the RFP available for review?

3.2 Will you be completing an assessment/Pilot/RFP phase, i.e. an evaluation by a vendor, 3rd party or your agency, of the current state, needs, & desired future state, in order to determine the cost, effort, approach and/or feasibility of a project?

No

3.2a Describe the reason for completing the assessment/pilot/RFP and the expected deliverables.

3.2b Provide the estimated cost, if any, to conduct the assessment phase and/or Pilot and/or RFP/solicitation process.

3.2e Based on research to date, provide a high-level cost estimate to implement the final solution.

4. PROJECT

4.1 Does your agency have a formal project methodology in place?

Yes

4.2 Describe the high level makeup and roles/responsibilities of the Agency, Vendor(s) and other third parties (i.e. agency will do...vendor will do...third party will do).

All IT development projects at the ASRS use the Agile-SCRUM methodology with a project manager, scrum master, product owner, software engineers and quality assurance engineers. The roles will be filled by a combination of FTE's and contractors. Currently all project manager roles are filled by FTE's.

Phase 5 of this project requires help from AZNET for the call center changes. They are the state's chosen vendor for the call center system and they are the only people authorized to make changes to it.

Phase 5 may also require a third party service to provide ANI number verification to pre identify the caller, which will result in ongoing operational costs for this service. The quote we received for this service is from TRUSTID. They are the currently favored vendor by AZNET.

4.3 Will a PM be assigned to manage the project, regardless of whether internal or vendor provided?

Yes

4.3a If the PM is credentialed, e.g., PMP, CPM, State certification etc., please provide certification information.

4.4 Is the proposed procurement the result of an RFP solicitation process?

No

4.5 Is this project referenced in your agency's Strategic IT Plan?

Yes

5. SCHEDULE

5.1 Is a project plan available that reflects the estimated Start Date and End Date of the project, and the supporting Milestones of the project?

Yes

5.2 Provide an estimated start and finish date for implementing the proposed solution.

Est. Implementation Start Date	Est. Implementation End Date
7/1/2019 12:00:00 AM	1/31/2023 12:00:00 AM

5.3 How were the start and end dates determined?

Based on project plan

5.3a List the expected high level project tasks/milestones of the project, e.g., acquire new web server, develop software interfaces, deploy new application, production go live, and estimate start/finish dates for each, if known.

Milestone / Task	Estimated Start Date	Estimated Finish Date
Phase 1: Modify FileNet and workflow to use PID	07/01/19	03/04/20
Phase 2: Replace PII within internal Applications	03/05/20	06/05/20
Phase 3: Create new FileNet document Class	06/08/20	02/23/21
Phase 4: Data Access Logs for POL system. Will allow us to track exactly who is doing what at the micro level.	02/24/21	08/01/22
Phase 5: Call Center Changes Modify IVR to not ask for SSN, possibly take advantage of ANI to verify authenticity of caller ID data for incoming calls.	08/02/22	01/11/23

5.4 Have steps needed to roll-out to all impacted parties been incorporated, e.g. communications, planned outages, deployment plan?

Yes

5.5 Will any physical infrastructure improvements be required prior to the implementation of the proposed solution. e.g., building reconstruction, cabling, etc.?

No

5.5a Does the PIJ include the facilities costs associated with construction?

No

5.5b Does the project plan reflect the timeline associated with completing the construction?

No

6. IMPACT

6.1 Are there any known resource availability conflicts that could impact the project?

No

6.1a Have the identified conflicts been taken into account in the project plan?

No

6.2 Does your schedule have dependencies on any other projects or procurements?

No

6.2a Please identify the projects or procurements.

6.3 Will the implementation involve major end user view or functionality changes?

Yes

6.4 Will the proposed solution result in a change to a public-facing application or system?

Yes

7. BUDGET

7.1 Is a detailed project budget reflecting all of the up-front/startup costs to implement the project available, e.g, hardware, initial software licenses, training, taxes, P&OS, etc.?

Yes

7.2 Have the ongoing support costs for sustaining the proposed solution over a 5-year lifecycle, once the project is complete, been determined, e.g., ongoing vendor hosting costs, annual maintenance and support not acquired upfront, etc.?

Yes

7.3 Have all required funding sources for the project and ongoing support costs been identified?

Yes

7.4 Will the funding for this project expire on a specific date, regardless of project timelines?

No

7.5 Will the funding allocated for this project include any contingency, in the event of cost over-runs or potential changes in scope?

Yes

8. TECHNOLOGY

8.1 Please indicate whether a statewide enterprise solution will be used or select the primary reason for not choosing an enterprise solution.

There is not a statewide enterprise solution available

8.2 Will the technology and all required services be acquired off existing State contract(s)?

Yes

8.3 Will any software be acquired through the current State value-added reseller contract?

No

8.3a Describe how the software was selected below:

8.4 Does the project involve technology that is new and/or unfamiliar to your agency, e.g., software tool never used before, virtualized server environment?

No

8.5 Does your agency have experience with the vendor (if known)?

Yes

8.6 Does the vendor (if known) have professional experience with similar projects?

Yes

8.7 Does the project involve any coordination across multiple vendors?

Yes

8.8 Does this project require multiple system interfaces, e.g., APIs, data exchange with other external application systems/agencies or other internal systems/divisions?

Yes

8.9 Have any compatibility issues been identified between the proposed solution and the existing environment, e.g., upgrade to server needed before new COTS solution can be installed?

No

8.9a Describe below the issues that were identified and how they have been/will be resolved, or whether an ADOA-ASET representative should contact you.

8.10 Will a migration/conversion step be required, i.e., data extract, transformation and load?

No

8.11 Is this replacing an existing solution?

No

8.11a Indicate below when the solution being replaced was originally acquired.

8.11b Describe the planned disposition of the existing technology below, e.g., surplused, retired, used as backup, used for another purpose:

8.12 Describe how the agency determined the quantities reflected in the PIJ, e.g., number of hours of P&OS, disk capacity required, number of licenses, etc. for the proposed solution?

A list of desired outcomes was gathered from senior management and the security team. Each item was discussed with senior developers and AZNET where the work was broken down into smaller tasks. These tasks were assigned a level of effort using story points. Each story point is equivalent to 50 hours of effort.

Hardware costs were provided by state approved vendor.

AZNET costs for IVR and call center modifications provided by AZNET.

ANI costs provided by AZNET's chosen ANI vendor "TRUSTID"

8.13 Does the proposed solution and associated costs reflect any assumptions regarding projected growth, e.g., more users over time, increases in the amount of data to be stored over 5 years?

Yes

8.14 Does the proposed solution and associated costs include failover and disaster recovery contingencies?

Yes

8.14a Please select why failover and disaster recovery is not included in the proposed solution.

8.15 Will the vendor need to configure the proposed solution for use by your agency?

Yes

8.15a Are the costs associated with that configuration included in the PIJ financials?

Yes

8.16 Will any app dev or customization of the proposed solution be required for the agency to use the project in the current/planned tech environment, e.g. a COTS app that will req custom programming, an agency app that will be entirely custom developed?

No

8.16a Will the customizations inhibit the ability to implement regular product updates, or to move to future versions?

8.16b Describe who will be customizing the solution below:

8.16c Do the resources that will be customizing the application have experience with the technology platform being used, e.g., .NET, Java, Drupal?

8.16d Please select the application development methodology that will be used:

8.16e Provide an estimate of the amount of customized development required, e.g., 25% for a COTS application, 100% for pure custom development, and describe how that estimate was determined below:

8.16f Are any/all Professional & Outside Services costs associated with the customized development included in the PIJ financials?

8.17 Have you determined that this project is in compliance with all applicable statutes, regulations, policies, standards & procedures, incl. those for network, security, platform, software/application &/or data/info found at aset.az.gov/resources/psp?

Yes

8.17a Describe below the compliance issues that were identified and how they have been/will be resolved, or whether an ADOA-ASET representative should contact you:

8.18 Are there other high risk project issues that have not been identified as part of this PIJ?

No

8.18a Please explain all unidentified high risk project issues below:

9. SECURITY

9.1 Will the proposed solution be vendor-hosted?

No

9.1a Please select from the following vendor-hosted options:

9.1b Describe the rationale for selecting the vendor-hosted option below:

9.1c Has the agency been able to confirm the long-term viability of the vendor hosted environment?

9.1d Has the agency addressed contract termination contingencies, e.g., solution ownership, data ownership, application portability, migration plans upon contract/support termination?

9.1e Has a Conceptual Design/Network Diagram been provided and reviewed by ASET-SPR?

9.1f Has the spreadsheet located at https://aset.az.gov/arizona-baseline-security-controls-excel already been completed by the vendor and approved by ASET-SPR?

9.2 Will the proposed solution be hosted on-premise in a state agency?

Yes

9.2a Where will the on-premise solution be located:

Agency's data center

9.2b Were vendor-hosted options available and reviewed?

No

9.2c Describe the rationale for selecting an on-premise option below:

All current applications that are being modified are currently located on our servers. Migrating these applications to other servers is not within the scope of this effort.

9.2d Will any data be transmitted into or out of the agency's on-premise environment or the State Data Center?

Yes

9.3 Will any PII, PHI, CGIS, or other Protected Information as defined in the 8110 Statewide Data Classification Policy be transmitted, stored, or processed with this project?

Yes

9.3a Describe below what security infrastructure/controls are/will be put in place to safeguard this data:

The systems we are changing already store the member's SSN and bank account numbers. The goal of this project is to reduce our use of SSN and bank account number by masking it or removing it where possible. The agency uses GAPP and NIST security controls to govern our use of PII.

10. AREAS OF IMPACT

Application Systems

Application Enhancements;Internal Use Web Application;New Application Development

Database Systems

Oracle

Software

Other

Internal Java based application (Public Employee Retirement Information System)

Hardware

Storage Area Network Devices

Hosted Solution (Cloud Implementation)

Security

Telecommunications

Telephone Upgrade - Business Specific

11. FINANCIALS

Description	PIJ Category	Cost Type	FY Spend	Qty	Unit Cost	Total Cost
TrustID ANI software as recommended by AZNET. $20,000 integration cost.	Professional & Outside Services	Development	1	1	$20,000	$20,000
Staff Augmentation Software Development year 1 Phase 1, Modify FileNet and workflow to use PID Phase 2, Replace PII within Applications	Professional & Outside Services	Development	1	1	$713,705	$713,705
ASRS FTE Software Development Cost, year 1 Phase 1, Modify FileNet and workflow to use PID Phase 2, Replace PII within Applications	Professional & Outside Services	Operational	1	1	$131,784	$131,784
Hard disk storage to accommodate data logging	Hardware	Development	2	1	$7,000	$7,000
ASRS FTE Software Development year 2 Phase 3, Create new FileNet Doc Class Start Phase 4, Data Access Logs	Professional & Outside Services	Development	2	1	$131,784	$131,784
Staff Augmentation Software Development year 2 Phase 3, Create new FileNet Doc Class Start Phase 4, Data Access Logs	Professional & Outside Services	Development	2	1	$713,705	$713,705
Staff Augmentation Software Development year 3 Phase 4 Data Access Logs continued Possibly Start Phase 5, Call Center Changes	Professional & Outside Services	Development	3	1	$713,705	$713,705
ASRS FTE Software Development Cost, year 3 Phase 4 Data Access Logs continued Possibly Start Phase 5, Call Center Changes	Professional & Outside Services	Operational	3	1	$131,784	$131,784
AZNET Professional services to modify IVR and API	Professional & Outside Services	Development	4	135	$134	$18,108
Yearly cost for ANI services from TRUSTID, $5,000 per month x 12 months. This is the cost of the ANI service during the project. NOTE: 3 year commitment required up front @ $180,000	Professional & Outside Services	Development	4	12	$5,000	$60,000
Staff Augmentation Software Development, year 4 Finish Phase 4 and 5	Professional & Outside Services	Development	4	1	$356,852	$356,852
AZNET Professional services to modify IVR and API buffer	Professional & Outside Services	Development	4	50	$135	$6,750
ASRS FTE Software Development Cost, year 4 Finish Phase 4 and 5	Professional & Outside Services	Operational	4	1	$65,892	$65,892

Base Budget (Available)	Base Budget (To Be Req)	Base Budget % of Project
$0	$0	0%
APF (Available)	**APF (To Be Req)**	**APF % of Project**
$0	$0	0%
Other Appropriated (Available)	**Other Appropriated (To Be Req)**	**Other Appropriated % of Project**
$0	$0	0%
Federal (Available)	**Federal (To Be Req)**	**Federal % of Project**
$0	$0	0%
Other Non-Appropriated (Available)	**Other Non-Appropriated (To Be Req)**	**Other Non-Appropriated % of Project**
$3,055,987	$0	100%

Total Budget Available	Total Development Cost
$3,071,068	$2,741,608
Total Budget To Be Req	**Total Operational Cost**
$0	$329,460
Total Budget	**Total Cost**
$3,071,068	$3,071,068

12. PROJECT SUCCESS

Please specify what performance indicator(s) will be referenced in determining the success of the proposed project (e.g. increased productivity, improved customer service, etc.)? (A minimum of one performance indicator must be specified)

Please provide the performance objective as a quantifiable metric for each performance indicator specified.
Note: The performance objective should provide the current performance level, the performance goal, and the time period within which that performance goal is intended to be achieved. You should have an auditable means to measure and take corrective action to address any deviations.
Example: Within 6 months of project completion, the agency would hope to increase "Neighborhood Beautification" program registration by 20% (3,986 registrants) from the current registration count of 19,930 active participants.

Performance Indicators

After project completion only a specific set of users will have access to view a person's full SSN and/or bank account number. Additionally each time this data is viewed the specific user who viewed it will be logged in a way that is easily reportable. Users without the permission to view the full SSN or bank account number will only be shown the masked SSN or bank account number.

All FileNet images will be indexed and retrieved by our internal users by using the member PID instead of member SSN

The Logging reports will provide the ability to answer the specific audit question: "Tell me exactly who accessed this member's data between this date range"

When someone calls into our call center they will not be asked to provide their SSN into the phone IVR in order to "pre identify" the caller for the agent.

13. CONDITIONS

Conditions for Approval

Should the final costs exceed the estimated costs by 10% or more, or should there be significant changes to the proposed technology, scope of work or implementation schedule, the Agency must amend the PIJ to reflect the changes and submit it to ADOA-ASET for review and approval prior to further expenditure of funds.

The Agency shall provide an informational update to the Information Technology Authorization Committee (ITAC) regarding the status of the project on an annual basis, or as otherwise requested.

14. ASET OVERVIEW

Project Background

An audit revealed security gaps within the internal systems used by the Arizona State Retirement System (ASRS). ASRS needs to limit the exposure of sensitive data by masking bank account information, including SSN's, for employees and potential hackers. Another weakness highlighted was their ability to track and log who was accessing sensitive information and when.

Business Justification

ASRS deals with sensitive data on a regular basis and any exposure would impact a large number of current and former State employees. The security measures outlined were chosen to address audit findings based on recommendations from RiskSense and Clifton Larson Allen Privacy Assessment

Implementation Plan

Development will be done internally using mixed teams of contractors and FTEs, many of whom are familiar with the existing systems. ASRS has broken development into phases and will use an agile/iterative approach. AZNet will also provide contracted support in the later phases of the project.

Vendor Selection

ASRS evaluated commercial off-the-shelf solutions and decided that the most cost-effective option was internal development teams made up of contractors and FTE's. AZNet will be involved in updating the systems they are currently involved with. AZNet also suggested an ANI vendor they have experience with, but the vendor will be re-evaluated if a new vendor is under contract with the State.

Budget or Funding Considerations

The cost of FTE's was included in the PIJ as an operational cost to better align with the related budget request and provide further visibility into the project. The estimated hours for software development being done by contractors is listed as a development cost for each fiscal year.

15. PIJ REVIEW CHECKLIST

Agency Project Sponsor

Anthony Guarino

Agency CIO (or Designee)

Kent Smith

Agency ISO (or designee)

Jeff Hickman

OSPB Representative

ASET Engagement Manager

Damon Wellman

ASET SPR Representative

Agency SPO Representative

Martha Rozen

Agency CFO