ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Application Security

HL23003

Department of Homeland Security

Contents

1. General Information

PIJ ID: HL23003
PIJ Name: Application Security
Account: Department of Homeland Security
Business Unit Requesting: Arizona Department of Homeland Security
Sponsor: Ngan Pham
Sponsor Title: Statewide Cybersecurity Program Manager
Sponsor Email: npham@azdohs.gov
Sponsor Phone: (480) 255-5706

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 State is currently lacking visibility into custom-developed applications, and effective mitigation solutions of security flaws in applications developed by its agencies and departments. This increases the risk of data breaches and other cybersecurity incidents. While application vulnerability assessments are periodically being conducted by either agencies that do them independently, hire contractors to do them, or are being provided by AZDOHS, that are not coordinated, and could miss coding flaws being introduced into mission critical business applications which may only be caught after an application is live in production.

As such, the Arizona Department of Homeland Security has been tasked with procuring and implementing an enterprise license for security software that will integrate security into the development process and scan software code in development, production, and postproduction to detect and reduce security risks by using at least two of the following testing mechanisms:

Static analysis security testing.

Dynamic testing.

Penetration testing.

Software composition analysis

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

Automate testing. Enables development teams to automate testing throughout the development lifecycle, performing an application control audit at various points to promote more secure software.

Accelerate development. By simplifying and speeding software testing, it enables development teams to meet deadlines for software builds.

Remediate faster. Application security software testing solutions provide step-by-step guidance for understanding, prioritizing and remediating vulnerabilities so developers can work more quickly to fix flaws.

Improve governance. Application security solutions enable organizations to adhere to web application security standards and establish processes for consistently delivering secure software.

2.3 Describe the proposed solution to this business need.

Veracode provides full end-to-end application security platform and developer training. This is StateRAMP approved. It is fully cloud native and has been deployed as a SaaS solution for over 15 years. It integrates application analysis into development life cycles and pipelines. It provides multiple security analysis technologies on a single platform, including static analysis, dynamic analysis, and software composition analysis, to find security vulnerabilities that include malicious code as well as the absence of functionality that may lead to security breaches.

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.

This is a SaaS solution.

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?

No

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).

AZDOHS- Responsible for vendor management and procurement of the technology solution. The Enterprise Control Tower will be the product owner of this solution and will provide support/assistance.

Vendor - Provide customer success manager(s) who holds PMP certification, customer success engineer, account executive, and solution architect. With the Customer Success Package VS-Premier Plus package, vendor will conduct program kick-off call, milestone & goal planning, program management consulting, DevSecOps/SDLC Design & Automation, Integrations, Plug-ins & APIs Support, policy & maturity workshops, end user product enablement, remediation coaching, mitigation reviews, program optimization review, compliance & governance reporting, Veracode Verified, Veracode Community, Support Initial response

State Agencies - Agency developers are responsible for their own application scanning, URL scanning, and participating in eLearning.

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?

No

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
5/18/2023 12:00:00 AM	10/31/2023 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
Schedule Kickoff Meeting	05/18/23	05/26/23
Technology Solution is procured	05/18/23	05/26/23
Create the Outcome Success Plan	05/22/23	06/02/23
Final Invoice Payment	06/01/23	06/30/23
Define Application Security Policy for scanning	06/05/23	06/09/23
Outreach to the five agencies that were on the Application Security Product Evaluation Committee to onboard and operationalize them on the platform	06/05/23	06/16/23
Review and prioritize applications needed to achieve the Plan	06/05/23	06/09/23
Outreach to all state agencies to identify which agencies want to utilize the platform	06/05/23	06/16/23
Create Rollout Plan, including end user training	06/12/23	10/31/23
Rollout Plan to each agency: Platform & Admin Setup & Training: Setup SAML (Optional); User Account Creation & Management; Application Profile Creation & Management; Analytics and Reporting	06/19/23	10/31/23
Complete Rollout Plan	06/19/23	10/31/23

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

No

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?

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

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?

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?

No

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

No

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?

Yes

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

No

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.

The project is using a statewide enterprise solution

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:

The Enterprise Security Program Advisory Council (ESPAC) stood up an Application Security Product Evaluation Committee with five members from five separate state agencies that develop their own applications. The Committee gathered technical and business requirements. A task order was sent out to vendors on statewide contracts to bring forward their vendors. Vendors that completed and passed the requirements document were invited to demo their solution. Demos were conducted. Statement of Works and quotes were evaluated. A vendor was selected based on the demos, passing the requirements, quotes, and statement of work.

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?

Yes

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

No

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?

No

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?

No

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?

We scoped to 500 developers/security engineers and 1,000 applications scanned. Veracode offered unlimited URLs scanned, unlimited application scanned, unlimited developers, and unlimited eLearning for developers.

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?

No

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?

No

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

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?

Yes

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

Commercial data center environment, e.g AWS, Azure

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?

No

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

No

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

No

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?

No

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

No

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

9.2b Were vendor-hosted options available and reviewed?

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

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

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?

No

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

10. Areas of Impact

Application Systems

Other

SaaS

Database Systems

Software

Hardware

Hosted Solution (Cloud Implementation)

Security

Other

Telecommunications

Enterprise Solutions

Other

11. Financials

Description	PIJ Category	Cost Type	Fiscal Year Spend	Quantity	Unit Cost	Extended Cost	Tax Rate	Tax	Total Cost
Static App, SCA, DYn, Elearn, Premier Plus, SeClabs-Dev	Software	Development	1	1	$1,603,603	$1,603,603	860.00 %	$137,910	$1,741,513
Static App, SCA, DYn, Elearn, Premier Plus, SeClabs-Dev	Software	Operational	2	1	$1,603,603	$1,603,603	860.00 %	$137,910	$1,741,513
Static App, SCA, DYn, Elearn, Premier Plus, SeClabs-Dev	Software	Operational	3	1	$1,603,603	$1,603,603	860.00 %	$137,910	$1,741,513
Static App, SCA, DYn, Elearn, Premier Plus, SeClabs-Dev	Software	Operational	4	1	$1,603,603	$1,603,603	860.00 %	$137,910	$1,741,513
Static App, SCA, DYn, Elearn, Premier Plus, SeClabs-Dev	Software	Operational	5	1	$1,603,603	$1,603,603	860.00 %	$137,910	$1,741,513

Base Budget (Available)	Base Budget (To Be Req)	Base Budget % of Project
$1,741,513	$0	100%
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**
$0	$0	0%

Total Budget Available	Total Development Cost
$1,741,513	$1,741,513
Total Budget To Be Req	**Total Operational Cost**
$0	$6,966,050
Total Budget	**Total Cost**
$1,741,513	$8,707,563

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

Within 30 days of procuring the application security solution, AZDOHS will identify all agencies interested in utilize the solution.

Get the first five agencies onboarded and utilizing the tool

Within 6 months of procuring the application security solution, 50% of agencies interested in utilizing the solution will have at least one application scanned, one URL scanned, and/or one developer participating in the eLearning.

Upon renewal of the application license, (May 2024), all agencies interested in utilizeing the solution will have a minimum of one application scanned, one URL scanned, and/or one developer using the eLearning platform.

13. Conditions

Conditions for Approval

Should development costs exceed the approved estimates 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, and ITAC if required, for review and approval prior to further expenditure of funds.

Monthly reporting on the project status is due to ADOA-ASET no later than the 15th of the month following the start of the project. Failure to comply with timely project status reporting will affect the overall project health. The first status report for this project is due on June 15, 2023.

14. Oversight Summary

Project Background

The Arizona Department of Homeland Security (AZDOHS) has a mission to safeguard the state by providing strategic guidance and access to resources for all stakeholders. AZDOHS objectives are to prevent terrorist attacks, strengthen border security, bolster cybersecurity efforts, decrease Arizona's susceptibility to all critical hazards, improve the ability and know-how to prepare for, mitigate, respond to, and recover from any critical hazards that impact Arizona.

Currently, the potential risk posed by custom-developed applications in the State is not entirely clear. Although application vulnerability assessments are being conducted, there is a possibility that coding errors may be introduced into essential business applications and not be detected. AZDOHS is responsible for acquiring and implementing software that will integrate security measures into the development process and scrutinize software code during development, production, and post-production stages which will identify and address security threats.

Business Justification

AZDOHS will utilize the Veracode solution to integrate with development tools, ensuring consistent enforcement of security policies across state Agencies. AZDOHS will have the ability to automate testing throughout the development lifecycle, facilitate application control audits at multiple points, and promote the development of more secure software. The solution will provide step-by-step guidance for understanding, prioritizing, and remedying vulnerabilities, help agencies adhere to web application security standards and establish processes for consistently delivering secure software, thereby improving governance. Veracode offers a full end-to-end application security platform and developer training, and is fully cloud native as a SaaS solution. It integrates application analysis into development pipelines, and provides multiple security analysis technologies on a single

platform, including static analysis, dynamic analysis, and software composition analysis, to find security vulnerabilities such as malicious code and the absence of functionality that may lead to security breaches.

Implementation Plan

AZDOHS will be responsible for vendor management and procurement of the technology solution. The Enterprise Control Tower will be the product owner of this solution and will provide support/assistance.

The vendor will be responsible for providing customer success manager(s) who hold PMP certification, customer success engineer, account executive, and solution architect. With the Customer Success Package VS-Premier Plus package, vendor will conduct program kick-off call, milestone & goal planning, program management consulting, DevSecOps/SDLC Design & Automation, Integrations, Plug-ins & APIs Support, policy & maturity workshops, end user product enablement, remediation coaching, mitigation reviews, program optimization review, compliance & governance reporting, Veracode Verified, Veracode Community, Support Initial response

Individual State Agency developers are responsible for their own application scanning, URL scanning, and participating in eLearning.

The project start, end and milestone dates will be adjusted once the vendor is awarded. The project timeframe will be the same duration as the PIJ approval.

Vendor Selection

AZDOHS received quotes from three vendors (Microfocus, SHI, WWT) and selected the vendor WWT due to their ability to provide unlimited application scanned, unlimited developers to utilize the platform, and unlimited training. WWT as the reseller and Carahsoft as the distributor offered the best and lowest costs.

Budget or Funding Considerations

Funding for the project consists of a 100% base budget.

15. PIJ Review Checklist

Agency Project Sponsor

Ryan Murray

Agency CIO (or Designee)

Agency ISO (or designee)

Ryan Murray

OSPB Representative

ASET Engagement Manager

ASET SPR Representative

Thomas Considine

Agency SPO Representative

Agency CFO