ADOA-ASET
Arizona Strategic Enterprise Technology

Project Investment Justification

Advanced Endpoint Protection - CrowdStrike

AD20006

Department of Administration

Contents

1. General Information

PIJ ID: AD20006
PIJ Name: Advanced Endpoint Protection - CrowdStrike
Account: Department of Administration
Business Unit Requesting: Enterprise Security
Sponsor: Tim Roemer
Sponsor Title: State Chief Information Security Officer
Sponsor Email: timothy.roemer@azdoa.gov
Sponsor Phone: (602) 542-2728

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…):

Advanced Endpoint Protection (AEP) was determined to be a critical enterprise security tool needed to prevent viruses on state computers by Enterprise Security Program Advisory Council (ESPAC) and National Institute of Standards and Technology (NIST). The existing contract is set to expire in October 2020, causing state computers to no longer have anti-virus protection. The ESPAC has a limited budget allocated to provide this security tool to the State Agencies. The State needed to identify a solution/tool within our existing budget that meets all technical requirements.

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

Advanced endpoint protection, protects systems from file, fileless, script-based and zero-day threats by using machine-learning or behavioral analysis. This keeps users endpoints (devices) safe from malicious content, in addition the solution will continuously monitor and record endpoint activity that will predict threat behavior; Provide visibility and blocking of malicious use of scripting tools such as Powershell, batch, bash; "Identify and block misuse of system utilities and other post-exploitation tools even after the tools have been altered to evade signature detection" and Provide near real-time alert generation.

2.3 Describe the proposed solution to this business need.

The multi-agency committee selected CrowdStrike to meet this need going forward because CrowdStrike met all requirements and has the potential to replace other tools as well. The State previously used Cylance as the AEP product and found, by using the CrowdStrike product, security professionals across the state will be able to protect their users endpoints at a cost savings compared to the existing tool.

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?

Yes

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

We have already completed a $0 Proof of Concept (POC) across multiple agencies. We did this to ensure that the security professional's technical requirements were met and that ADOA's requirements for multi-tenancy and visibility were met. The POC was successful and allowed the State to try multiple products and select the one that best met their needs.

We will be purchasing off existing state contracts, so there is no cost for POC.

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

0

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

200000

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).

ADOA - Configure and deploy client to agency. Manage tool at the Enterprise level.

Agencies - Configure and deploy client to their agency. Give access to additional users via Role Based Access Control (RBAC).

Vendor - Create initial users and agencies in console. Provide technical support to ADOA and agencies during configuration phase. Provide support after initial deployment.

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
5/18/2020 12:00:00 AM	10/28/2020 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
Deliverable: Migration Communications Plan	05/18/20	05/22/20
Deliverable: Create deployment plan	05/26/20	05/29/20
Deliverable: Create training plan	06/01/20	06/05/20
Train Admins	06/08/20	06/12/20
Deploy to 80% of Agencies	06/08/20	10/28/20

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?

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?

Yes

8.3a Describe how the software was selected below:

A multi-agency committee drafted the requirements and viewed demos from 9 vendors on contract. Initial pricing was requested from 5 vendors. Based on initial pricing, two vendors were selected for POC. A two-month POC was conducted at 10+ agencies to test the products and compare functionality. Their recommendation was taken to the ESPAC. ESPAC agreed and supported their recommendation to select CrowdStrike.

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?

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?

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?

Yes

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

2016 - original contract CStor ADSPO16-137340. This is a new OTS software.

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

Both the existing and new solutions are licenses. We will be removing the clients installed and installing new clients for the new product.

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 have used 36,000 licenses for all Enterprise Security tools. We have our current utilization.

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?

No

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

Not needed

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?

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?

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

Database Systems

Software

COTS Application Acquisition

Hardware

Hosted Solution (Cloud Implementation)

Security

Security Controls/Systems - Other

Advanced Endpoint Protection - Enterprise Tool

Telecommunications

Enterprise Solutions

Other

11. Financials

Description	PIJ Category	Cost Type	Fiscal Year Spend	Quantity	Unit Cost	Extended Cost	Tax Rate	Tax	Total Cost
Software licenses for CrowdStrike Platform Pro	Software	Development	1	36000	$4	$153,000	815.00 %	$12,470	$165,470
Technical Support	Professional & Outside Services	Development	1	1	$23,477	$23,477	0.00 %	$0	$23,477
Software Licenses for CrowdStrike Platform Pro	Software	Operational	2	36000	$4	$153,000	815.00 %	$12,470	$165,470
Software licenses for CrowdStrike Platform Pro	Software	Operational	3	36000	$4	$153,000	815.00 %	$12,470	$165,470
Software Licenses for CrowdStrike Platform Pro	Software	Operational	4	36000	$4	$153,000	815.00 %	$12,470	$165,470
Software Licenses for CrowdStrike Platform Pro	Software	Operational	5	36000	$4	$153,000	815.00 %	$12,470	$165,470

Base Budget (Available)	Base Budget (To Be Req)	Base Budget % of Project
$850,825	$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
$850,825	$188,947
Total Budget To Be Req	**Total Operational Cost**
$0	$661,878
Total Budget	**Total Cost**
$850,825	$850,825

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

State will have the ability to block 80% of malicious content sent to end user devices via automation.

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.

14. Oversight Summary

Project Background

ADOA-ASET currently has a contract for Advanced Endpoint Protection (AEP) with the vendor Cylance for licenses to protect state computers against viruses. The contract will end October 2020 leaving state equipment vulnerable to malicious scripting tools such as Powershell, batch, and bash.

Business Justification

The agency found comparable Advanced Endpoint Protection can be purchased at a price that is less than the cost of the current Advanced Endpoint Protection resulting in drastic cost savings for the state, less viruses on state computers, and less data breaches.

Implementation Plan

The project will be completed 5 months from the start date. The agency will be responsible for the configuration and deployment of the solution.
The vendor will be responsible for creating initial users and agencies in console and providing technical support during configuration and deployment.

Vendor Selection

Nine vendors provided demos to 10+ agencies, and five vendors provided quotes. The vendor CrowdStrike was selected based on the product functionality requirements by multiple agencies and the cost savings.

Budget or Funding Considerations

The project will be funded by 100% base budget appropriated by the security budget for the security program available every July 1 and set to expire June 30 of each fiscal year.

The purchase of licenses will not be when the project starts, this will happen later in the project due to work needing to be done before purchasing the licenses.

15. PIJ Review Checklist

Agency Project Sponsor

Tim Roemer

Agency CIO (or Designee)

JR Sloan

Agency ISO (or designee)

Tim Roemer

OSPB Representative

ASET Engagement Manager

ASET SPR Representative

Thomas Considine

Agency SPO Representative

Eric Bell

Agency CFO

Derik Leavitt