Project Investment Justification

Insider Threat Risk Management

AD18016

Department of Administration

1. GENERAL INFORMATION

PIJ ID: AD18016
PIJ Name: Insider Threat Risk Management
Account: Department of Administration
Business Unit Requesting: ASET-Security
Sponsor: Mike Lettman
Sponsor Title: State Chief Information Security Officer (CISO)
Sponsor Email: mike.lettman@azdoa.gov
Sponsor Phone: (602) 542-0030

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 function of the State of Arizona governmental agencies is to serve the citizens of Arizona. Citizens trust the State with personal information, health information, financial information, and more. The State endeavors to safeguard this information and to protect it from any unintended consequences.

To that end, ADOA-ASET has an Enterprise Security team that is responsible for administering a suite of security controls that helps protect the State's IT systems, applications, networks, devices, and other assets.

ADOA-ASET follows the National Institute of Standards and Technology (NIST) Cybersecurity framework, which recommends a number of controls with the purpose of assessing and improving the State's ability to prevent, detect, and respond to cyber attacks. The Enterprise Security team currently oversees and manages a suite of 14 enterprise solution controls (out of a potential 20), and now seeks to deploy three additional enterprise security controls to fill existing gaps that place the State at risk.

While the existing 14 controls deployed protect against known "external" threats, the State lacks a comprehensive enterprise approach to effectively address the growing "insider" threats. Thus, State data continues to be at risk, as most Agencies do not currently have solutions capable of monitoring and defending against insider threats.

Insider threats in cyber security are often associated with malicious users, but employees and/or contractors can inadvertently cause a data breach. A prime example would be a loss of credentials due to phishing or theft. Another example is when an employee, through carelessness, invites malware into the system by clicking on a link in a spam email or unknowingly bringing an infected device to work. Other honest mistakes include sending sensitive files to the wrong address. All of these are only a small list of ways in which employees can inadvertently compromise State data and cost the State money.

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

This project will provide cost effective, best in class, enterprise security insider threat control solutions across State agencies which will help protect against cyber-attacks and data ex-filtration. The project will primarily utilize cloud-hosted solutions, and will take advantage of enterprise purchasing power to negotiate lower per-seat pricing.

These standardized enterprise security solutions deployed throughout the State will enable agencies to effectively address insider threats, while allowing collaboration and sharing of threat information at a lower cost of ownership.

This project aligns directly with ADOA-ASET's Strategic Goal of "Secure the Enterprise" and has indirect impacts on the RiskSense Security Goals, as this enterprise project helps transform and improve the way the State manages cyber security. This approach allows for consistent application of industry best practices through strategically sourced enterprise tools and services that enhance the speed, reduces costs, and increases the effectiveness of cyber security procurements.

2.3 Describe the proposed solution to this business need.

The three additional controls that are being added to the portfolio of Enterprise Security products were selected after extensive research and discovery and include:

Cloud Access Security Broker (CASB): Acts as an intermediary between "us and the cloud". Existing security measures applied to on-premise solutions are extended to cloud services, preventing any gaps in security between cloud and on-premise solutions.

User and Entity Behavior Analytics (UEBA): Collects and analyzes the behavior of users, groups and devices to establish baselines and identify unusual behaviors. By learning what is considered normal behavior, the solution makes it possible to detect and identify security risks and threats when abnormal actions are performed.

Phishing: Sends emails to employees with fake links, mimicking real phishing attempts from outside threats. Employees who are tricked into clicking on simulated links are required to complete security awareness training.

Please see Budget or Funding Considerations listed in Engagement Manager section for funding explanation.

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.

For each of the solution areas (CASB, UEBA, Anti-Phishing), the project team researched solutions that were known as viable options through research articles, Gartner's Magic Quadrant, other state and agency experiences, and from the CISO's/sponsor's recommendations.

Approximately 20 vendors were evaluated, and the best of those were brought in for presentations across the three solutions and benchmarked against initial requirements.

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.

4054632

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-ASET IT Governance Steering Committee inc. State CIO - review and approval of business case

- ADOA-ASET Security team - providing technical expertise and technical project leads

- ADOA-ASET EPMO- providing Project management and project coordination support

- State Chief Information Security Officer (CISO) - sponsor

- Participating Agency IT staff - providing vendor review and developing requirements

- State Compliance and Privacy Officer - providing security reviews and approvals

- ADOA/SPO Officer - providing solicitation and contractor selection support

- State Contractors - State network equipment and services contract vendors

- Vendors - with ITRM solutions work with State contractors

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
8/1/2018 12:00:00 AM	6/30/2019 12:00:00 AM

5.3 How were the start and end dates determined?

Other

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

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?

Yes

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?
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.
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:

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)?
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?

Yes

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?

Estimated quantities are made based on the number of State of Arizona FTE/contractors and devices and prior experience with similar projects. Planning for future fiscal years may include an expansion of these controls, along with additional security controls after more research is completed.

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?

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:
In line with Cloud first strategies and goals

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

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

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?
Yes

9.3a Describe below what security infrastructure/controls are/will be put in place to safeguard this data:
Vendors will complete AZRamp process and data will be encrypted; also, if solution is not in AWS or Azure, the moderate impact baseline security controls will be completed.

10. AREAS OF IMPACT

Application Systems

Database Systems

Software

Hardware

Hosted Solution (Cloud Implementation)

Security
Security Controls/Systems - Other

Telecommunications

Enterprise Solutions

Contract Services/Procurements

11. FINANCIALS

Description	PIJ Category	Cost Type	Fiscal Year Spend	Quantity	Unit Cost	Extended Cost	Tax Rate	Tax	Total Cost
Phishing License/Maintenance & support (Yr 1 and 2)	License & Maintenance Fees	Development	1	64000	$1	$88,960	805.00 %	$7,161	$96,121
UEBA - Configuration Support	Professional & Outside Services	Development	1	1	$132,000	$132,000	0.00 %	$0	$132,000
UEBA -License & Support Services 30,001 to 40,000 users (24 mths)	License & Maintenance Fees	Development	1	1	$1,268,000	$1,268,000	795.00 %	$100,806	$1,368,806
CASB - License and Support (Yr 1 & 2)	License & Maintenance Fees	Development	1	32000	$44	$1,400,000	795.00 %	$111,300	$1,511,300
CASB-License and Support (Yr 3)	License & Maintenance Fees	Operational	3	32000	$25	$800,000	795.00 %	$63,600	$863,600
Phishing License/Maintenance & Support (Yr 3)	License & Maintenance Fees	Operational	3	32000	$1	$44,480	805.00 %	$3,581	$48,061

Base Budget (Available)	Base Budget (To Be Req)	Base Budget % of Project
$0	$0	0%
APF (Available)	**APF (To Be Req)**	**APF % of Project**
$3,108,227	$0	77%
Other Appropriated (Available)	**Other Appropriated (To Be Req)**	**Other Appropriated % of Project**
$0	$911,661	23%
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
$3,108,227	$3,108,227
Total Budget To Be Req	**Total Operational Cost**
$911,661	$911,661
Total Budget	**Total Cost**
$4,019,888	$4,019,888

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

Deploy 3 Insider Threat tools to 96 Executive Branch Agencies at 80% adoption by June 30, 2019.

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.

There are three Security Controls identified in this PIJ: Phishing, Cloud Access Security Broker, and User and Entity Behavior Analytics. The vendor names are abstracted for security purposes, but if any of the controls are changed or the vendors are replaced, ADOA-ASET must inform ITAC of their intent to make a change.

14. ENGAGEMENT MANAGER COMMENTS

Project Background

In order to assist with protecting the computers, networks, equipment, and information assets of the State of Arizona, ASET-SISPO (Statewide Information Security & Privacy Office) has currently deployed 14 IT security controls to ensure systems and data are protected. These 14 controls are primarily geared towards mitigating the threat from external attack vectors, Following due diligence with the State Procurement Office (SPO), this Project Investment Justification documents acquisition of three additional security controls: 1) Cloud Access Security Broker; 2) User and Entity Behavior Analytics; and 3) Phishing.

Business Justification

The new Controls being acquired will help close gaps in the overall security posture of the State by focusing on internal threats. The three additional controls that are being added to the portfolio of Enterprise Security products were selected after extensive research and discovery and include:

Cloud Access Security Broker (CASB): Acts as an intermediary between “us and the cloud”. Existing security measures applied to on-premise solutions are extended to cloud services, preventing any gaps in security between cloud and on-premise solutions.

User and Entity Behavior Analytics (UEBA): Collects and analyzes the behavior of users, groups and devices to establish baselines and identify unusual behaviors. By learning what is considered normal behavior, the solution makes it possible to detect and identify security risks and threats when abnormal actions are performed.

Phishing: Sends emails to employees with fake links, mimicking real phishing attempts from outside threats. Employees who are tricked into clicking on simulated links are required to complete security awareness training.

Implementation Plan
ASET-SISPO (Statewide Information Security & Privacy Office) has provided Oversight with an implementation plan and a Project Manager has been assigned to the acquisition and deployment. The installation and deployment of the three new solutions varies. Phishing is an application that will be pushed to all local devices. The other two solutions (UEBA and CASB) are cloud solutions that do not need local installations. Implementation will be completed by June 2019 to all agencies. Proofs of concept and testing have already been completed.

Vendor Selection
The first step in the selection process was to determine what types of security controls were missing from the portfolio of Enterprise Security products already in place. Multiple agencies were involved in the requirements gathering. After the gaps were identified and attack vectors understood, vendors that offered solutions that met the State's needs were then identified. Vendors were asked to provide demonstrations and some were tested under a proof of concept.
Approximately 20 vendors were initially evaluated on price, features, and level of effort to implement, and ultimately 3 were selected that best served the State's needs.

Budget or Funding Considerations
ADOA received favorable review in December 2017 for 14 existing security controls. ADOA is seeking favorable review for an additional 2.9 million in June 2018 to pay for the three new controls. The remaining $250,000 will be coming from the existing security budget approved in December 2017. No operational funds will be required.

15. PIJ REVIEW CHECKLIST

Agency Project Sponsor
Mike Lettman

Agency CIO (or Designee)
Morgan Reed

Agency ISO (or designee)
Mike Lettman

OSPB Representative

ASET Engagement Manager
Joel Munter

ASET SPR Representative

Agency SPO Representative

Agency CFO