

# CHANGE REQUEST / AMENDMENT

## PIJ ID AD18016 - Insider Threat Risk Management

Arizona Department of Administration

**5-Year Lifecycle Budget Estimate:**

Total Development Budget	\$ 3,108,227
<u>Total Operational Budget</u>	<u>\$ 911,661</u>
Total Overall Budget	\$ 4,019,888

**Areas Affected:**

End Date	No
Development Costs	No
Scope	Yes

Original End Date: 06/30/2019

Revised End Date: No Change

**Change Description:**

**CURRENT AMENDMENT 01: 4/17/19**

The Insider Threat Risk Management Project Investment Justification (PIJ) was approved with conditions by ITAC on July 18, 2018. The project encompassed implementing and deploying three new tools to safeguard against insider threats - both malicious and accidental.

- Cloud Access Security Broker (CASB) is a cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.
- Phishing is a tool that allows the organization to safely send test emails to their employees to determine if they are susceptible to phishing scams. There is a training component that helps employees understand how to better identify potentially malicious emails and prevent State Data and employee credentials from being inappropriately released or compromised.
- User and Entity Behavior Analytics (UEBA) models and identifies typical and atypical behavior of humans and machines within a network. This is done using large volumes of network and security log data. By identifying normal behavior patterns, it becomes easier to identify activities outside of that pattern. Once these activities are identified, the response can range from monitoring the activity to automatically denying access to sending alerts. All of the responses are governed by rules and policies that are completely customizable. By identifying the threat earlier, the State can limit the exposure and mitigate the risk sooner.

**With this current Change Request**, the Department of Administration requests approval to amend the original scope from having the solution hosted in the State’s AWS presence to be hosted in the State’s Data Center. This change is requested to remain within the original project budget and increase sustainability. This scope change has no impacts to the current development costs.

**Financial Detail:**

**Original PIJ Financials 7/18/18 ITAC**

<i>Five Year Life-Cycle Summary</i>						
<i>Cost Description</i>	<i>FY2019</i>	<i>FY2020</i>	<i>FY2021</i>	<i>FY2022</i>	<i>FY2023</i>	<i>Total</i>
Development Costs	\$3,108,277	\$0	\$0	\$0	\$0	3,108,2771
Operational Costs	\$0	\$0	\$911,661	\$0	\$0	\$911,668
Total Project Costs	\$3,108,277	\$0	\$911,661	\$0	\$0	\$4,019,888

# CHANGE REQUEST / AMENDMENT

PIJ ID AD18016 - Insider Threat Risk Management

Arizona Department of Administration

## Amended PIJ Financials 4/17/19 ITAC

<i>Five Year Life-Cycle Summary</i>						
<i>Cost Description</i>	<i>FY2019</i>	<i>FY2020</i>	<i>FY2021</i>	<i>FY2022</i>	<i>FY2023</i>	<i>Total</i>
Development Costs	\$3,108,277	\$0	\$0	\$0	\$0	\$3,108,277
Operational Costs	\$4,500	\$14,400	\$926,061	\$14,400*	\$926,061*	\$1,885,422
Total Project Costs	\$3,112,777	\$14,400	\$926,061	\$14,400	\$926,061	\$4,993,699

\* *Notes on Budget:*

- *The total project cost includes a \$973,811 increase in operational costs. There is no increase in development cost.*
- *Renewals for products will be re-evaluated in FY2022 and FY2023. If products are not renewed, additional operational costs will not be needed.*