Multnomah County

Program #78318B - IT Cyber Security 6/25/2019

Department: County Assets **Program Contact:** Tracey Massey

Program Offer Type: Innovative/New Program **Program Offer Stage:** As Adopted

Related Programs:

Program Characteristics: One-Time-Only Request

Executive Summary

This program is to enhance our Cyber Security posture at Multnomah County. Over the past 3 years we have worked diligently to achieve our Cyber Security goals and have been able to significantly increase our cyber posture. The additional funds in our Cyber Security 2.0 program offer will allow us to continue our progress to address gaps and deficiencies that have been identified by both internal and third party reviews.

Program Summary

From ransomware to DDoS attacks, threats have multiplied to the point where we can no longer say perimeter defenses like firewalls are enough. We need to know when our assets are behaving strangely on the network. There's no faster way to detect anomalies than real-time analytics with wire data. Acquiring this capability will enable us to proactively hunt for threats, analyze and understand user behavior to identify anomalies and identify and address devices that should not be on our network. This program will address the following:

Second layer authentication: This program will improve information security by adding a second layer of authentication to select County applications. This project will initially focus on building the technical and organizational infrastructure for County employees with elevated privileges to use this service. This lays the groundwork for required implementation by key applications and populations in the successive phases.

Network Access Control: With the increase of network activity on our “industrial network” (doors, security, heating and cooling, etc) we are at greater risk of experiencing a breach in that environment due to the fact that the environment is largely not understood or defined. Network Access Control can help us to understand what should and should not be on our network and restrict what these devices are able to access based on rules that we define.

Privileged Access and Identity Management: Privileged access is the access most often targeted by cyber security threats because this access leads to the most valuable and confidential information. Implementing a Privileged Access and Identity Management solution will allow us to have better control in managing and securing privileged accounts to meet the needs of the access control requirement for a number of the compliance regulations.

Performance Measures

Measure Type	Primary Measure	FY18 Actual	FY19 Purchased	FY19 Estimate	FY20 Offer
Output	Completion of multi-factor authentication.	NA	NA	NA	100%
Outcome	Targeted systems identified and dual-factor authentication has been implemented effectively.	NA	NA	NA	100%

Performance Measures Descriptions

Output - Technology tool identified, procured, and ready for deployment.
Outcome - Top systems identified and multi-factor authentication implemented.

Legal / Contractual Obligation

Revenue/Expense Detail

	Proposed General Fund	Proposed Other Funds	Proposed General Fund	Proposed Other Funds
Program Expenses	**2019**	**2019**	**2020**	**2020**
Contractual Services	$0	$0	$0	$468,020
Total GF/non-GF	**$0**	**$0**	**$0**	**$468,020**
Program Total:	**$0**		**$468,020**	
Program FTE	0.00	0.00	0.00	0.00

Program Revenues				
Financing Sources	$0	$0	$0	$468,020
Total Revenue	**$0**	**$0**	**$0**	**$468,020**

Explanation of Revenues

Revenue is one-time-only funding from the Information Technology fund.

Significant Program Changes

Last Year this program was: