Multnomah County

Program #78318 - IT Cyber Security

6/30/2016

Department: County Assets **Program Contact:** Bob Leek

Program Offer Type: Existing Operating Program **Program Offer Stage:** As Adopted

Related Programs:

Program Characteristics: One-Time-Only Request

Executive Summary

This Program Offer is a carryover request. Several aspects of the County's cybersecurity components are in process of being addressed. The efforts include replacement of the County's obsolete firewall (the primary network defense system that protects the County from external cyber threats); replacement of the end of life email security monitoring and archiving service; development of a County security awareness training program; and implementing tools dedicated to the management of data and systems in the cloud.

Program Summary

Several efforts were initiated in FY2016. The firewall analysis and re-architecture plan was completed. Vendor product demos, final product selection, procurement and implementation will be completed in FY2017.

Security improvement work and vulnerability remediation for a critical business system was completed in FY2016.

The email security monitoring and archiving projects have completed the vendor demo and product selection phase. The contracting phase is underway and will be completed in FY2016, with the purchase and implementation of the selected products completed in FY2017.

Efforts planned for FY2017 include a security awareness training program for the County staff and procuring and implementing tools dedicated to the management and monitoring of our systems in the "cloud" and in our physical data center.

County staff are both our front line of defense as well as the last mile in our protection strategy. The security awareness program is a resource that will educate our staff on not only what they can do to reduce malicious activity, but also how to detect and resist attacks. Over the past few years, County IT has made a strategic decision to embrace a "cloud-first" strategy. As we move data between systems internally and externally, we need to be able to identify and classify data hosted in these environments, then monitor to identify malicious activity or anomalous behavior and provide scalable protections for those activities.

Performance Measures

Measure Type	Primary Measure	FY15 Actual	FY16 Purchased	FY16 Estimate	FY17 Offer
Output	% of project completion for firewall, email archiving and retention	N/A	75%	40%	100%
Outcome	Firewall system is supported by vendor and patches are up to date.	N/A	100%	100%	100%

Performance Measures Descriptions

PM #1 Output - This measure is designed to ensure a secure, redundant firewall system is fully implemented and operational.
PM #2 Outcome - This measure is designed to ensure our firewall system is patched at their current levels.

Legal / Contractual Obligation

Revenue/Expense Detail

	Proposed General Fund	Proposed Other Funds	Proposed General Fund	Proposed Other Funds
Program Expenses	**2016**	**2016**	**2017**	**2017**
Contractual Services	$0	$0	$0	$1,091,197
Materials & Supplies	$0	$1,155,000	$0	$175,413
Capital Outlay	$0	$570,000	$0	$0
Total GF/non-GF	**$0**	**$1,725,000**	**$0**	**$1,266,610**
Program Total:	**$1,725,000**		**$1,266,610**	
Program FTE	0.00	0.00	0.00	0.00

Program Revenues				
Financing Sources	$0	$1,725,000	$0	$1,266,610
Total Revenue	**$0**	**$1,725,000**	**$0**	**$1,266,610**

Explanation of Revenues

This program will use FY 2016 one-time only General Funds.

Significant Program Changes

Last Year this program was: FY 2016: 78037-16 Cyber Security

The ongoing nature of changes in the threats to our cybersecurity capabilities require identifying those threats and establishing mitigation plans related to those vulnerabilities. The initial work identified for FY2016 is under way, and new items have been identified and will be addressed with in FY2017. Continued viligence and planning are expected as an ongoing component of this program offer. Requesting FY2016 carryover to continue the project completions in FY2016.