Multnomah County

Program #78318 - IT Cyber Security

4/18/2018

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

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

Related Programs:

Program Characteristics: One-Time-Only Request

Executive Summary

This Program Offer requests carries forward a number of the County's multi-year cybersecurity programs and projects that are currently in process. The efforts include the replacement of the County's legacy firewall platform (the primary network defense system that protects the County from external cyber threats); replacement of the end of life email security monitoring service; development of a County security awareness training program; and implementing tools dedicated to the monitoring and management of data and systems in the cloud and in the data center(s).

Program Summary

The new Fortinet firewall platform and accompanying SPLUNK log management and analysis tool have been implemented and configured for production. Firewall migration to the new Fortinet platform is in progress and will carryover into FY 2019. The data center fabric redesign, purchase and implementation portion of the project will begin in Q4 FY 2018 and implementation will carryover into FY 2019.

In FY 2018 County IT purchased (SPLUNK), a tool that allows the county to share infrastructure data to enable the correlation of activities inside of the county's systems. County IT also formalized and standardized our HIPAA incident response by purchasing and implementing a decision support tool called RADAR. This tool provides the ability to apply the same logic to each incident and obtain consistency in determining if there has been a breach. The Cyber Security awareness program was also expanded and received Chair's Office approval to make cyber security training mandatory for all employees beginning January 2018.

In FY 2018, VIRTRU was purchased and implemented. This tool has improved how we protect and encrypt email. It has greatly simplified the process and adds an additional layer of protection that detects protected or sensitive information and will prompt the user to add encryption to the message. Also, currently in process to be purchased and implemented in FY 2018 are two other tools, Tenable and DMARC. Tenable will used be used to address our vulnerability scanning and reporting of physical and IoT devices, which addresses the Federal HIPAA requirement for continuous monitoring and mitigation of system vulnerabilities. DMARC is an email-validation system designed to detect and prevent email spoofing.

In FY 2019, the focus will be on DNS (Domain Name Service), network anomaly detection and cloud security through data encryption, access, logging and monitoring.

Performance Measures

Measure Type	Primary Measure	FY17 Actual	FY18 Purchased	FY18 Estimate	FY19 Offer
Output	Purchase, install and migrate to new firewall platform to meet growing capacity, security and technological needs.	N/A	N/A	N/A	100%
Outcome	Next generation firewall in production	75%	100%	100%	100%
Output	Purchase and installation of Enterprise Email Filtering Technology	N/A	N/A	N/A	100%
Outcome	End User Awareness Program - reduction in the number of potential security incidents as a result of users clicking	N/A	N/A	N/A	12%

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 the firewall system addresses the security and operational needs of the county.
PM #3 Output - This measure is designed to add a level of protection to our email system that did not previously exist.

Legal / Contractual Obligation

Revenue/Expense Detail

	Proposed General Fund	Proposed Other Funds	Proposed General Fund	Proposed Other Funds
Program Expenses	**2018**	**2018**	**2019**	**2019**
Contractual Services	$0	$791,669	$0	$515,599
Total GF/non-GF	**$0**	**$791,669**	**$0**	**$515,599**
Program Total:	**$791,669**		**$515,599**	
Program FTE	0.00	0.00	0.00	0.00

Program Revenues				
Beginning Working Capital	$0	$791,669	$0	$515,599
Total Revenue	**$0**	**$791,669**	**$0**	**$515,599**

Explanation of Revenues

This program will carryover unspent one time only revenues into FY 2019 as beginning working capital through project completion.

Significant Program Changes

Last Year this program was: FY 2018: 78318 IT Cyber Security

The ongoing nature of changes in the threats to our cyber security capabilities require identifying those threats and establishing mitigation plans related to those vulnerabilities. Continued diligence and planning are expected as an ongoing component of this program offer. Requesting FY 2018 carryover to continue the project completions in FY 2019.