COLLIN COUNTY

Information Technology
2300 Bloomdale Rd
Suite 3198
McKinney, Texas 75071
www.collincountytx.gov

To: Judge Keith Self
Commissioner Fletcher
Commissioner Williams
Commissioner Hill
Commissioner Webb
Bill Bilyeu

From: Caren Skipworth, IT Director

Date: 05/01/2017

Re: Request for “Open DNS Project” approval and Budget Amendment

The Information Technology Department would like to request approval from Commissioner’s Court to utilize savings from completed “EOL Switch/Router Replacement Project”, Project Code#: P06008 to cover funding for “Open DNS Project” in the amount of $130,000.00. This project has been requested in the FY2018 Budget, but if approved now to use the left over funds from the “EOL Switch/Router Replacement Project” the request will be removed from the FY2018 Budget.

FY2018 Budget - Program Improvement Information:

Current situation: Currently Collin County resolves internet addresses by querying the Root DNS servers on the internet. While this works, it provides an attack vector for hackers to use to compromise the county network. The issue is that hackers will often spin up thousands of new domain names with domain generation algorithms (DGA) when attempting to compromise networks. For example in January 2017 a county computer was compromised and attempted to go to the following website “nlbejmccbhkncgokjcmghpfloaajcffj.com” to phone home and receive instructions. This domain was spun up the same day the computer was compromised so the county’s existing services that use internet reputation failed to identify the threat. This happens because the sites are so new and random that there is no reputation yet.

Detailed description: This request is to purchase the cloud service Cisco Umbrella Insights and Investigate for three years (formally Open DNS). This service will handle all DNS request from the county and will shield us by not allowing malicious connections to be made out to command and control servers. Cisco Umbrella will immediately improve Collin County’s security profile in multiple ways. It will improve security by blocking newly seen domains for a period of time so reputation services can be built up. Cisco Umbrella has also developed algorithms to identify DGAs and block them. Because this service handles 80 billion requests a day it quickly converges on bad acting domains and has the ability to predict those domains before they are confirmed as a problem. While no service is, 100% and network security has to be done as a layered approach Cisco Umbrella will do this by stopping malicious communication before it can be started.

Please note that there is no requirements pending that requires the project to begin before FY2018 adopted budget.

Caren Skipworth with the Information Technology Department will be available for questions.