File #: 20-640, **Version:** 1

Broward County Commission Regular Meeting
Director's Name: George Tablack
Department: Finance and Administrative Services **Division:** Purchasing

Information

Requested Action
MOTION TO APPROVE sole brand, sole source standardization of Splunk Inc. for Information and Event Management software solution to mitigate security attacks against multiple systems and applications within Broward County, utilizing the most appropriate alternate government contract at the time of contract execution, for Enterprise Technology Services Division, including all Broward County agencies and offices.

Why Action is Necessary
In accordance with the Broward County Procurement Code, Section 21.54.c, the Board is required to approve all standardizations over the award authority of the Director of Purchasing; and Section 21.43, the Board is required to approve all contracts for supplies or services of more than five years.

What Action Accomplishes
Standardize Splunk Inc. security information and event management enterprise security platform which provides visibility to investigate security incidents in real time.

Is this Action Goal Related
Yes

Previous Action Taken
None.

Summary Explanation/Background
THE FINANCE AND ADMINISTRATIVE SERVICES DEPARTMENT AND THE PURCHASING DIVISION RECOMMEND APPROVAL OF THE ABOVE MOTION.

This item supports the Board's Value of "Consistently delivering responsive, efficient, quality services to the public and internal customers"; and its Goal to "Build into every process and service effective checks and balances that do not cause inefficiency, but rather ensure consistency, continuity, and quality".

Splunk is the County's primary security monitoring and alerting system. It has been integrated with the County's ERP system at implementation of PeopleSoft as a sole brand purchase on July 30, 2015. Splunk has been proven to be compatible within the County infrastructure and systems. Splunk offers a cost-effective and flexible way to meet compliance requirements including audit trail collection, monitoring, and reporting into a single solution to help assess the County’s security

profile.

Separate systems would cause organizational data silos, data collection issues, scalability challenges and complete lack of analytic capabilities including correlated alerts. Without County-wide analytic capabilities, the County's solution would be severely degraded and put the County at significant risk. Splunk routinely has logged over 40+ billion events for the County, overall improving the County's data security posture.

Splunk Inc. (Splunk) produces software for searching, monitoring, and analyzing machine-generated big data via a Web-style interface. Splunk Log Management Enterprise Security solution monitors and provides security audit logs identifying user access times, source of login and network activity logs. Splunk is used by the Enterprise Technology Services (ETS) Division as a log management and security information and event management system that provides a central repository for collecting and monitoring data from multiple systems and applications across Broward County. Splunk provides consistency for operational support and satisfies regulatory and industry log management standards such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) compliance guides.

Splunk provides:

- Real-time central visibility across the County's information security systems
- Seamlessly integrates with the following County systems:
  - Cloud ERP system (PeopleSoft)
  - Windows servers
  - Firewalls and security systems
  - Databases
  - Applications
- Event log management solution that consolidates data from numerous sources to assist in secured business continuity
- A correlation of events gathered from different logs or security sources, using logic rules that add intelligence to raw data
- Automatic security event notifications and visualized dashboards for investigating security issues
- Faster response and triage of security incidents

Upon standardization, the Broward County Aviation Department (BCAD) seeks to follow the County standard currently being utilized by ETS. This ability will expand BCAD incident response capabilities. In the event there is a compromise, the logs will be used to investigate the potential incident.

The County currently utilizes U.S. General Services Administration (GSA) Schedule No. GS-35F-0119Y. The County's annual usage is estimated at $350,000. Splunk sole brand usage to date is $361,349.

ETS has reviewed this request and concurs with this recommendation (Exhibit 2).

Source of Additional Information

Brenda J. Billingsley, Director, Purchasing Division, (954) 357-6070

Fiscal Impact

Fiscal Impact/Cost Summary

There is no fiscal impact for this action.