DATE: September 09, 2019

TO: Brenda J. Billingsley, Director, Purchasing Division

THRU: Michael Nonnemacher, Aviation Chief Operating Officer

FROM: Angela Scott, Information Systems Administrator, Aviation Department

PROJECT TITLE: Splunk Cloud Subscription for Aviation

REQUISITION NO. AVI-

SOLE SOURCE/SOLE BRAND REQUEST

I. REQUEST: Provide a description of the features of the product/service or Scope of Work.

Broward County Aviation Department (BCAD) is requesting a sole brand designation for the log management product Splunk Enterprise with Splunk App for Enterprise Security. BCAD seeks to be included on the master agreement TEC2117443G1_1 to purchase licenses through the existing Enterprise Technology Services (ETS) contract with Presidio Networked Solutions LLC.

BCAD seeks to follow the County standard currently being used by ETS. Splunk Enterprise with Splunk App for Enterprise Security is one of the industry-leading platforms for Security Information and Event Management. The solution has the ability to correlate with several mission critical applications/systems at Aviation. ETS has had great success with Splunk, which in the past has logged over 40+ billion events for the County, overall improving their information and data security posture. Some examples of security and audit logs used by ETS include user access times, source of login, and network activity logs. This ability will be very important in expanding BCAD incident responses capabilities. Splunk provides actionable intelligence that will help prioritize threats and will foster the ability to act fast in response to a discovered threat. In the event there is a compromise, the logs will be used to investigate the potential incident. This solution provides visibility to investigate security incidents in real time and is a paramount tool in a successful security management program.

II. JUSTIFICATION: Please check all boxes that describe your reason(s) for determining that only one source or brand is reasonably available.

Only Sole Source/ Uniqueness

☐ Proprietary Item - this vendor/source has the only rights to provide this service or commodity. A letter from the manufacturer or authorizing entity is included in this request.

☐ Technology Improvements - updates or upgrades to an existing system, software, software as a service (SaaS), hardware purchases.

☐ Engineering Direction - engineering drawing or specification identifies product; "no substitutes or equivalents will be acceptable."

☐ Only qualified supplier - reliability and maintainability of the product or service would be degraded unless specified supplier is used; may void warranty. This request includes a copy of the current warranty information.

☑ Other/or Additional information - the County requires this sole source, sole brand purchase for the following reasons:

Splunk was procured by ETS as the County standard for Security Information and Event Management (SIEM). After investigation and liaison with ETS, Splunk was found as the best-fit product to meet BCAD's

log management needs.

After initial investigations, Splunk already has the ability to integrate with the following app/add-ins in the Aviation environment: Cisco Security Suite, Splunk Add-on for Cisco ASA, Cisco Firepower App for Splunk, SolarWinds Add-on for Splunk, Windows Event Logs Analysis, Splunk DB Connect, Malwarebytes Visibility and Dashboards, Technical Add-on for Malwarebytes, Splunk App for PCI Compliance - Splunk Enterprise, Nessus Data Importer, Splunk App for Microsoft SharePoint, Splunk Add-on for Websense DLP, HP Printer Security, AlgoSec App for Security Incident Analysis and Response, Splunk Add-on for IBM WebSphere Application Server, Splunk Add-on for NetFlow, and Maximo App for Splunk.

Business Case (One/Most Reasonable Source or One/Most Reasonable Brand)

- ☐ Operational Compatibility - replacement parts from alternate suppliers are not interchangeable with original part and causes equipment incompatibility. Previous findings and/or documentation is included with this request.
- ☐ Ease of Maintenance - maintenance or retooling prohibits competition. Section III, Comparative Market Research includes estimated costs associated with changing current source and/or brand.
- ☐ Follow-On - potential for continued development or enhancement with same supplier and eliminates costs incurred by using different supplier. Section III, Comparative Market Research includes estimated costs for replacing current or existing system.
- ☐ Complies with existing community and safety standards, and/or laws, rules, and regulations.
- ☐ Exempted from the Procurement Code - per Section 21.18 of Broward County Administrative Code.
- ☑ Other/or additional information - using this sole source, sole brand purchase benefits the County for the following reasons:

With guidance and lessons learned from ETS, BCAD will have the ability to expedite the learning curve involved in the implementation and adaption of a product of the nature, ultimately further assisting in creating safer technology environments for BCAD stakeholders. Without a robust solution that provides automation, analytics, and end-to-end viability into our security posture BCAD could be put at significant risk.

III. COMPARATIVE MARKET RESEARCH: Provide a detailed source or market analysis for justification of sole source/brand or most reasonable source (attach extra sheets as needed).

Estimated project value: 200,000.00 Contract length (if applicable): 3 years

Expenses to date: 0

Has this commodity or service been previously provided to the County? ◉ Yes ○ No

If yes, when and by whom? ETS

How was item/service procured? Sole brand

What is the current contract (MA) or purchase order number? TEC2117443G1_1

If this is a sole brand, is there an "authorized" dealers list? ○ Yes ◉ No

Cost/Benefit Analysis: What would the cost be to utilize an alternate vendor or source? This explanation should include the savings and/or additional costs to the County by not using the preferred vendor or source. Attach additional sheets if needed.

BCAD is committed to rising to the challenge of protecting our stakeholders and commitment to a Security Information and Event Management (SIEM) including log management, which is imperative to a robust cyber and information security defense strategy. BCAD desires to align with the current County standard set by ETS allowing for a smoother system transitions and better utilization of staff's time and efforts.

Splunk is not the only SIEM on the market, which can collect logs from multiple devices. Multiple vendors are able to collect raw data and save to a repository. However, Splunk is recognized as being specialized in these abilities and would offer BCAD economies of scale for integration that could be lost if another product is selected.

CERTIFICATION: I have thoroughly researched the sole source or sole brand justification and fully understand the implications of Section 838.22 of the Florida Statutes:

(2) "It is unlawful for a public servant, with corrupt intent to obtain a benefit for any person or to cause unlawful harm to another, to circumvent a competitive bidding process required by law or rule by using a sole source contract for commodities or services."

(5) "Any person who violates this section commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084"

Angela Scott	Angela Scott Digitally signed by Angela Scott DN: dc=local, dc=fll-airport, ou=FLLUSERS, cn=Angela Scott Date: 2019.09.09 09:25:52 -04'00'	September 9, 2019
REQUESTOR/EVALUATOR (PRINT)	REQUESTOR/EVALUATOR (SIGN)	DATE
Michael Nonnemacher	Michael Nonnemacher Digitally signed by Michael Nonnemacher DN: dc=local, dc=fll-airport, ou=FLLUSERS, cn=Michael Nonnemacher Date: 2019.09.10 10:22:42 -04'00'	September 9, 2019
DEPT/DIV DIRECTOR OR DESIGNEE (PRINT)	DEPT/DIV DIRECTOR OR DESIGNEE (SIGN)	DATE

The Purchasing Agent has reviewed the request and has completed the required due diligence per the Procurement Code Section(s) 21.34 and 21.35. The Purchasing Agent recommends the following:

☐ Sole Source ☑ Sole Brand ☐ Reasonable Source ☑ RFI attached ☐ Rejected

☐ Request Authorization to Negotiate

Additional Information:

Splunk Enterprise collects index logs from technology infrastructure, security systems and business applications by collecting index logs and machine data in databases utilizing and enterprise-class architecture supporting hundreds of terabytes of data per day. ETS utilizes Splunkbase applications and add ons to enhance and extend the splunk platform. The agent of concern recommends Board standardization of all Splunk product suites so agencies may determine the best splunk solutions meeting agency needs. ETS utilizes Splunk Enterprise solution while Aviation intends to implement a Splunk Cloud-based solution. This will give the agencies the flexability to utilize the optimum solution that meets their environment's needs.

Purchasing Agent Signature: LEAHANN LICATA Digitally signed by LEAHANN LICATA Date: 2019.12.06 16:40:35 -05'00' Date: 12/6/19

DAVID CLEMENTE Digitally signed by DAVID CLEMENTE Date: 2019.12.10 14:30:12 -05'00'

APPROVAL AUTHORITY

REASON/SUGGESTED ACTION (IF DISAPPROVED):

Signature: BRENDA BILLINGSLEY Digitally signed by BRENDA BILLINGSLEY Date: 2020.01.09 12:51:33 -05'00' Date:

DATE: May 18, 2018

TO: Brenda J. Billingsley, Director, Purchasing Division

THRU: John Bruno, Chief Information Officer, Enterprise Technology Services Division

FROM: Benjamin Sanchez, IT Business Services Director, Enterprise Technology Services Division

PROJECT TITLE: Sole Brand procurement for Splunk

REQUISITION NO. ETS0001135

SOLE SOURCE/SOLE BRAND REQUEST

I. REQUEST: Provide a description of the features of the product/service or Scope of Work.

Enterprise Technology Services (ETS) is requesting a sole brand designation for the log management product Splunk Enterprise with Splunk App for Enterprise Security. The current master agreement MA023A1334704G1 expires on July 30, 2018. ETS seeks to create a new master agreement to purchase additional licenses and convert existing licenses. Splunk has changed their licensing agreement to term versus perpetual, which is what we utilize today. Since our contract will terminate in FY'19, in addition to the extra sizing, yearly term licenses need to be purchased for the overall solution, eliminating any capital expense requirements, but increasing the yearly recurring operating expense.

Splunk Enterprise with Splunk App for Enterprise Security is one of the industry-leading platforms for Security Information and Event Management. This solution has been used to correlate all ETS managed systems security event logs for the past 3 years logging over 40 billion events to date.
Some examples of security and audit logs are: user access times, source of login, and network activity logs. In the event there is a compromise, the logs will be used to investigate a breach. This solution provides visibility to investigate security incidents in real time. It offers the ability to categorize user transactions, customer activity, machine behavior, security threats, and fraudulent activity. The solution correlates logs from multiple devices using machine learning to alert the County of potential security events.

II. JUSTIFICATION: Please check all boxes that describe your reason(s) for determining that only one source or brand is reasonably available.

Only Sole Source/ Uniqueness

- ☐ Proprietary Item - this vendor/source has the only rights to provide this service or commodity. A letter from the manufacturer or authorizing entity is included in this request.
- ☐ Technology Improvements - updates or upgrades to an existing system, software, software as a service (SaaS), hardware purchases.
- ☐ Engineering Direction - engineering drawing or specification identifies product; "no substitutes or equivalents will be acceptable."
- ☐ Only qualified supplier - reliability and maintainability of the product or service would be degraded unless specified supplier is used; may void warranty. This request includes a copy of the current warranty information.
- ☐ Other/or Additional information - the County requires this sole source, sole brand purchase for the following reasons:

Business Case (One/Most Reasonable Source or One/Most Reasonable Brand)

☐ Operational Compatibility - replacement parts from alternate suppliers are not interchangeable with original part and causes equipment incompatibility. Previous findings and/or documentation is included with this request.

☐ Ease of Maintenance - maintenance or retooling prohibits competition. Section III, Comparative Market Research includes estimated costs associated with changing current source and/or brand.

☐ Follow-On - potential for continued development or enhancement with same supplier and eliminates costs incurred by using different supplier. Section III, Comparative Market Research includes estimated costs for replacing current or existing system.

☐ Complies with existing community and safety standards, and/or laws, rules, and regulations.

☐ Exempted from the Procurement Code - per Section 21.18 of Broward County Administrative Code.

☑ Other/or additional information - using this sole source, sole brand purchase benefits the County for the following reasons:

Splunk was procured via a sole brand purchase on July 30th, 2015. A sole brand purchase for Splunk was used because of the results of an RFI (R1252905F1) ETS submitted. The RFI demonstrated Splunk was the best fit for Broward County. Log Management solutions do not normalize all logs out of the box. All solutions need custom configuration to completely utilize different types of customer logs. Our current installation has indexed over 40 billion events to date. Over the past three years ETS has been able to normalize logs from many different sources using various resources such as professional services, training classes, conferences, and individual research. In some cases, on-boarding these logs required downtime as configurations were modified. Splunk alerting is utilized County wide by various agencies such as ETS, Port Everglades, Parks, Traffic Engineering, and ERP.

Currently, Sierra Cedar sends all logs from PeopleSoft to the County using the Sierra Cedar Splunk log forwarder (ERP Master Services Agreement, Exhibit B-2 Payment Schedule on page 8 states Sierra Cedar uses the Splunk Auditing Service). ETS is able to use the County installation to receive, maintain, monitor, and analyze the County PeopleSoft logs. If ETS moved to a different SIEM, a separate installation of Splunk would have to be maintained to continue receiving PeopleSoft logs from Sierra Cedar. ETS would be required to have two isolated monitoring systems. This would leave the County at risk and decrease the effectiveness of the two solutions. Two separate systems would cause organizational data silos, data collection issues, scalability challenges and complete lack of analytics capabilities including correlated alerts. Without County wide analytic capabilities the solution would be severely degraded and put the County at significant risk.

III. COMPARATIVE MARKET RESEARCH: Provide a detailed source or market analysis for justification of sole source/brand or most reasonable source (attach extra sheets as needed).

Estimated project value: $375,000 Contract length (if applicable): 3

Expenses to date: $190,638

Has this commodity or service been previously provided to the County? ◉ Yes ○ No

If yes, when and by whom? Carahsoft

How was item/service procured? Sole brand

What is the current contract (MA) or purchase order number? MA023A1334704G1

If this is a sole brand, is there an "authorized" dealers list? ◉ Yes ○ No

Cost/Benefit Analysis: What would the cost be to utilize an alternate vendor or source? This explanation should include the savings and/or additional costs to the County by not using the preferred vendor or source. Attach additional sheets if needed.

ETS has devoted a significant amount of resources for the purchase of this solution. Attempting to switch the current log management solution to an alternate vendor would incur significant costs and create a transition period of loss of security team resources and County investment thereby creating cyber risk to the County.

The initial costs are not recurring and would have to be paid again if the County went to a new solution (hardware, and installation services). ETS invested over two months in on-site professional services and technical support tickets for configuration and initial setup. For three weeks alone two full time employees were dedicated to this configuration. Following the configuration and intial setup, significant hours were invested by various subject matter experts from the Datacomm, Linux, and Server teams. Several hours of planned downtime had to be coordinated months in advance for a successful implementation. Additionally, two weeks of professional services cost $25,000 during the engagement.

From a training standpoint, ETS Security team has attended multiple off-site Splunk conferences gaining significant insight and enhancements to real world scenarios. Two full time employees attended the official 4-Day Splunk conference for approximately $5,000. This conference helped add various reports, alerts, and dashboards specific to Splunk to strengthen the County's security posture and lower the risk of cyber attacks and data breaches. Furthermore, the team was able to learn from multiple technical sessions enhancing our efficiency of the product. Over the last three years ETS has purchased and attended over 10 training classes to enhance the teams overall knowledge and productivity on the solution. These classes took multiple weeks where security team members were dedicated to learning the product.

Splunk is not the only SIEM on the market which can collect logs from multiple devices. Multiple vendors are able to collect raw data and save to a repository. Although to have a real-time understanding of what is happening and deep analysis of what has occured across our systems, all of our devices must have specific fields mapped to a common variable. Our current Splunk infrastructure has collected over 40 billion events from over 150 devices. To be able to correlate and normalize logs which map fields between different devices takes considerable time, customization, testing, and downtime. ETS has invested hundreds of hours configuring these devices to be able to streamline and efficiently correlate events from different device sources. If ETS has to migrate to a new SIEM, the implementation would require months of planning, months to develop and configure custom connectors for each device, months of report and alert conversions, and months of learning a new SIEM architecture and console. ETS would have to run concurrent systems contributing to escalating costs due to redundant hardware, dwindling efficiency, reduced security team resources, and additional service and application downtime. While the system is being migrated, ETS would have months of limited visibility into systems, leaving the County at significant risk.

ETS is requesting the Sole Brand procurement of a Splunk subscription for 300 gigabytes per day of software usage for Splunk Enterprise, and Splunk Enterprise Security.

CERTIFICATION: I have thoroughly researched the sole source or sole brand justification and fully understand the implications of Section 838.22 of the Florida Statutes:

(2) "It is unlawful for a public servant, with corrupt intent to obtain a benefit for any person or to cause unlawful harm to another, to circumvent a competitive bidding process required by law or rule by using a sole source contract for commodities or services."

(5) "Any person who violates this section commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084"

Ben Sanchez		Digitally signed by BENJAMIN SANCHEZ Date: 2018.05.15 15:35:38 -04'00'	May 15, 2018
REQUESTOR/EVALUATOR (PRINT)	REQUESTOR/EVALUATOR (SIGN)		DATE
John Bruno		Digitally signed by JOHN BRUNO Date: 2018.05.15 18:15:44 -04'00'	May 15, 2018
DEPT/DIV DIRECTOR OR DESIGNEE (PRINT)	DEPT/DIV DIRECTOR OR DESIGNEE (SIGN)		DATE

The Purchasing Agent has reviewed the request and has completed the required due diligence per the Procurement Code Section(s) 21.34 and 21.35. The Purchasing Agent recommends the following:

☐ Sole Source ☑ Sole Brand ☐ Reasonable Source ☐ RFI attached ☐ Rejected

☐ Request Authorization to Negotiate

Additional Information:

The purchasing agent recommends the Splunk Enterprise solution as a sole brand for the Splunk License Support and Maintenance for the Enterprise Technology Services Division (ETS). Splunk Enterprise Security Software was purchased by ETS in 2015 to provide required security monitoring logs for integration with Sierra-Cedar's EFP environment. In the ERP Master Services Agreement, Exhibit B-2 Payment Schedule on page 8 states Sierra-Cedar uses the Splunk Auditing Service and that is their log management tool. To switch the current log management solution to an alternate vendor the County would incur significant costs and create a transition period of loss of security team resources and County investment thereby creating cyber risk to the County.
Based on an RFI (R1252905F1) from August 20th, 2014, Splunk was the best fit for Broward County.
The Purchasing agent recommends continuing the piggy-back contract utilizing GSA Schedule No: GS-35F-0119Y (between State of Florida and Carahsoft Technology Corporation) or GSA Schedule No: 47QTCA18D00A9 (between State of Florida and EPIC MACHINES, INC.) to the end of the GSA contract expiring December 19, 2021 to ensure continuation of maintenance and support.

Purchasing Agent Signature: ECATERINA SULI-WOLF Digitally signed by ECATERINA SULI-WOLF DN: dc=cty, dc=broward, dc=bc, ou=Organization, ou=BCC, ou=PU, ou=Users, cn=ECATERINA SULI-WOLF Date: 2018.09.05 16:00:57 -04'00' Date: LEAHANN LICATA Digitally signed by LEAHANN LICATA DN: dc=cty, dc=broward, dc=bc, ou=Organization, ou=BCC, ou=PU, ou=Users, cn=LEAHANN LICATA Date: 2018.09.05 16:08:44 -04'00'

APPROVAL AUTHORITY

REASON/SUGGESTED ACTION (IF DISAPPROVED):

Signature: GLENN MARCOS

Digitally signed by GLENN MARCOS
DN: dc=cty, dc=broward, dc=bc, ou=Organization, ou=BCC, ou=PU, ou=Users, cn=GLENN MARCOS
Date: 2018.09.19 17:36:32 -04'00'

Date: 9/19/18