UNIVERSITY OF SOUTH CAROLINA

AMENDMENT NO.1 TO SOLICITATION

TO: ALL VENDORS

FROM: Kevin Sanders, Procurement Manager

SUBJECT: SOLICITATION NUMBER: USC-IFB-2400-KS
Security Event Management (*SIEM*) software and hardware and Enterprise Incident Response software

DATE: April 22nd , 2013

This Amendment No.1 modifies the Invitation for Bid only in the manner and to the extent as stated herein.

Opening date is extended to 5.7.13 at 2:30pm
Award will be posted on 5.9.13

Vendor Questions/Answers

BIDDER SHALL ACKNOWLEDGE RECEIPT OF AMENDMENT NO.1 IN THE SPACE PROVIDED BELOW AND RETURN IT WITH THEIR BID RESPONSE. FAILURE TO DO SO MAY SUBJECT BID TO REJECTION.

_____ _____
Authorized Signature Name of Offeror

_____
Date

USC SEIM IFB

Will USC allow for responses and an award of LOT 1 and LOT 2 independent of the other, or must respondents respond to both LOTs?

Independent

Will USC consider a Security as a Service model that meets the requirements of the bid as opposed to a Software/Hardware Package?

Yes

~respectfully requests an extension to submit the offer from 4/30/13, 2:30 P.M. to 5/7/13, 2:30 P.M.

LOT 1.

Bullet 1. Is the requirement that a proposed SEIM solution utilize these open source tools or that the SEIM solution has the ability to receive logs from those systems?

It must have the ability to manage the profile of the scan and kickoff scans within the interface of the tool. Also it should limit the IP space allowed to scan based on the roles of the defined user.

Bullet 2. Please indicate the live IP devices that will be scanned. Is this Active Scanning both internal and external or external only?

50K IP's. Internal only scan.

Bullet 3. Is the bid requesting threat management or log management or both?

It should be able to do both.

Bullet 4. Please define OSSEC or confirm as OSSEC HIDS and the version. **http://www.ossec.net/.**

We have agents running 2.5-2.7.

Bullet 5. Provide version of SNORT and Suricata.

The most current version and keep it updated within a week of release.

Bullet 7. How many Netflow CPE devices and what is the aggregate bandwidth of those devices? What is the average bandwidth utilization of those devices?

At this time, we are not implementing this feature but want the product to have the capability to be able to if desired.

Bullet 8. Provide a list of other systems that need to be monitored. Device monitoring is typically not a function of a SEIM solution. Is USC willing to allow third party vendor management so that monitoring is achieved?

No third party vendor. This portion will not be implemented for the University, but a small subset of critical devices that have limited access. The SEIM should be the only console needed to check Availability of these devices.

Bullet 15. Please define long term?

8 Years for only system that need to meet this requirement.

I have a question regarding Solicitation #USC-IFB-2400-KS “Security Event Management (SIEM) software and hardware and Enterprise Incident Response”

Will these items need to be included in Lot #1 in the license line item #1?

- Provide a hardware appliance with support
- Provide implementation support for the solution
- Provide onsite training to a minimum of five people

For the reference, can I include the references from the manufacturer since the support and training will be delivered directly from the manufacturer?

Yes, supply reference material from manufacturer