Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

REQUEST FOR PROPOSAL #2020-028
Network Data Analytics Platform
RESPONSE ADDENDUM #02
December 12, 2019

QUESTIONS

1. Could you please elaborate on the Requirement #1?
   What exactly is meant by BGP Analytics? Is this about receiving AS information via flow records and providing visualization/reporting/analysis using this information?
   Answer: Yes, the level of BGP integration is for data augmentation tocorrelate flow data with path information. Describe the level of BGPintegration provided by your solution in your response, if applicable.

2. Regarding Requirement #21?
   Do you have a preference for a virtual, physical, or on-prem solution? Can we submit variations of the solution in the same submittal?
   Answer: We prefer a cloud-based solution or an on-prem, physical, turn-key solution. You may delineate variations of your solution within your proposal.

3. Regarding Requirement #21?
   For cloud hosted architecture, it is assumed that the data must be sent over secured connection. What are the supported secure connections for your flow sources?
   Answer: We will entertain encrypted as well as traditional, non-encrypted, netflow collection at this time.

4. Regarding Requirements 30-33?
   Can you detail the traffic growth (fps) over the timeline of the deployment? We want to be able to create the best overall TCO and not design for the maximum from year 1.
   Answer: We expect to export approx. 40K fps year one, with modest year over year growth. Capacity may need to increase in response to other changes in networking monitoring requirements.

5. How many users will be accessing the system at the same time?
   Answer: Generally, fewer than 10, typically 1 to 3.

6. Regarding Requirements #34 and 35
   Answer: Here is a textual description of a sample query of typical complexity that we expect to execute within the time limits described for unsampled data (as described below) or for sampled data (substitute “over the last 4 weeks”):

   “Display the for top N source IP (version 4) and destination TCP-port pairs, selecting only source IPs from University IP address space, and selecting only destination IPs from outside the University IP address space, and only those with the SYN flag set, and among them those representing the highest number of distinct destination IPs over the last 24 hour period ”

7. How many networking devices to collect data from? ie. Cisco & nprobe count. Counted by IP sourcing flow data, switch stack or HA pair with vIP =1 device. Can you provide some examples of the queries?
   Answer: nprobe - 10 (currently 8), cisco - 4

8. Time for a technical PoC does not seem to be included in the current timeline. Is there going to be time set aside for a fair evaluation, if no, why not?
   Answer: Yes - The announcement date is subject to change. We reserve time to technically evaluate promising proposals before a final announcement is made.

9. Regarding RFP requirement #14: can we please get clarity on thevagueness of 'Describe the capabilities of the proposed system's netflow analysis' ?
   Answer: The proposed solution shall be able to analyze raw netflow ingested from our sensors/devices, and provide higher level analytic capabilities. This would include aggregating like flows based on selected criteria, e.g. flows with the same source IP , or same dest IP, or same source/dest TCP port, specific combination of TCP flags (e.g. SYN or ACK but not PSH), or the most packets sent to remote networks, or to identify the pair of IPs exchanging the most flows per second.