**Requirements Document – R184559 - Purchase of LogRhythm Security Information Event Manager (SIEM)**

Item 1: XM6410 w/ 1000 MPS License - (Hardware appliance for installation in the CoM data center, initially licensed and configured to capture 1000 messages per second (MPS). Appliance has the capability to scale up to 5000 MPS with additional licensure.)

Item 2: AIE Server License 5000 MPS License - (Analytics engine, providing advanced AI and machine learning to analyze the logged data. Licensure is based on maximum capacity of the hardware appliance.)

Item 3: 2 Day of Professional Services - (Installation and configuration services.)

Item 4: 1 Seat Virtual Instructor-Led End User Training - (Join LogRhythm for an online hosted, virtual training presentation of the LogRhythm CORE training topics. Each virtual training allows customers to join a virtual classroom hosted by a Certified LogRhythm Trainer for a full-day online training of the LogRhythm End User or Administrator training courses. Each participant will receive an electronic copy of corresponding LogRhythm Training Services Course Material, and a Virtual Training Environment to be used with other participants and LogRhythm Instructor. Hard copies of the training material can be purchased for an additional fee. Classes run from 9am MST to 5pm MST. )

Item 5: 10 System Monitor Lite standard agents -

- Available on Windows, Linux, Solaris, HP-UX and AIX, individual System Monitor Agents are capable of collecting from hundreds of devices and deliver
- Centralized Management
- SSL Encrypted Communication
- Guaranteed Collection
- 10:1 Data Compression for Transportation
- Remote Data Aggregation
- Time Stamp Normalization
- Scheduled Collection
- TCP Forwarding
- Host Activity Monitoring
- Independent Process Monitor Network Connection Monitor
- User Activity Monitor
- Data Loss Defender

Item 6: 5 System Monitor Pro advanced agents -

- In addition to functionality available with LogRhythm's System Monitor Agents, the following advanced features are available with the System Monitor Pro
- Cisco IDS – SDEE format
- Checkpoint – OPSEC LEA
- Flow Data

SNMP

Vulnerability Data

File Integrity Monitoring

Detect reads, modifications and deletions

Identify specific user or application

Unidirectional Communications for Classified Environments

Integration with one-way data diodes

Support for classified/top secret deployment

Item 7: First year maintenance and support standard business (includes all Software and Hardware Support)

- Contact our support team during standard business hours, Monday – Friday, 7am – 6pm MT (Mountain Time)
- Access to software updates, including all major and minor releases and LogRhythm Knowledge Base updates
- 4-hour response to technical support requests, during standard support hours
- Next business day delivery of replacement hardware in the event of unresolvable equipment issues, during standard support hours