Question No.	RFP Section	Question	UMGC Response
1	Section I. General Information	*For RFP #91804 Firewall Hardware, Software and Related Support & Services, would* <UMGC> *accept MEEC Hardware Contract 2017, UMD-972016? <...> Or MEEC IT Security Services & Solutions* <?>	No, UMGC will not utilize the MEEC contract for the basis of award. UMGC will establish a contract based on the submission requirements in RFP #91804.
2	Section III. Procurement Phases and Evaluation Process; Paragraph 3. HECVAT LITE	*Does* <a prospective proposer> *as a reseller need to fill out the HECVAT for this RFP? It appears that a lot of the questions in that tool are not really specific to* <prospective proposer> *being a reseller, but more as the actual product owner.*	Any Offeror who is requested to provide the HECVAT LITE will be expected to fill out the HECVAT LITE irrespective of whether or not they are a reseller. Pursuant to Section III. Article 1. Paragraph 3 on page 13 of the RFP document, the HECVAT LITE is NOT required to be submitted with the Technical Proposal. A copy of the HECVAT LITE is provided in Appendix D for Offerors to review. Offerors will be requested, via addendum, to complete the HECVAT LITE by the specified due date listed in the addendum. The HECVAT LITE is a questionnaire that is specifically designed for higher education institutions to measure vendor risk. The purpose is for the Offeror to submit robust security safeguard information regarding the product and service being proposed by the Offeror to the University.
3	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.1 states: "Four (4) firewalls to be configured in high-availability pairs in two (2) separate locations". Requirement 2.1.3.4 states: "Each firewall unit must be able to cluster HA pairs of firewalls across geographically distributed data centers". *Does UMGC desire the separate locations to perform as a single "virtual firewall" with high availability?* *If so, is there a layer 2 interconnection and what is the available bandwidth between sites?*	No, each cluster will be in one location. Cluster 1 (two firewalls) will be in location 1 and cluster 2 (two firewalls) will be in location 2.
4	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.2.1 states: "Each firewall unit must provide the following: Firewall throughput of at least 56 Gbps". Requirement 2.1.3.4 states: "Each firewall unit must be able to cluster HA pairs of firewalls across geographically distributed data centers". *For this requirement (as well as the other performance-related requirements), is the full throughput required for the overall system given the loss of any one member in the cluster, or for any given site, or for any given firewall at a given site?*	The full throughput is for each firewall.
5	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.2.4 states: "Each firewall unit must provide maximum sessions of at least 50 M". *Is this meant to mean 50,000,000 (50 Million)?*	Yes, this means 50,000,000 (50 Million).

Question No.	RFP Section	Question	UMGC Response
6	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.2.5 states: "Each firewall unit must provide support for 20 to 24 10 Gig SFP+ interfaces". *Would aggregated higher speed physical interfaces (40 Gbps or 100 Gbps) with sub-interfaces be an acceptable offer? If not, could an offer include additional adjacent switches to provide the requested total number of physical interfaces?* *Given that the existing firewalls each have 3 physical interfaces (reference requirements 2.3.2.1 and 2.3.2.2 in the Scope of Work in the RFP document) are the additional required interfaces for future growth purposes?*	The firewall must support up to 20-24 physical interfaces, with a minimum requirement of 8 physical interfaces. The physical interface speed should be 40Gbps and support 10Gbps (current infrastructure). We are currently using 3 interfaces. The remaining are for future growth.
7	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.3.1 states: "Each firewall unit must be capable of at least 25 Gbps of SSL Inspection throughput measured with IPS enabled, and HTTP traffic using TLS v1.2 AES256-SHA". *Should <prospective proposers> understand "SSL Inspection" to mean full SSL decryption? If so, does UMGC have an existing solution performing such features including the necessary PKI system to decrypt and re-sign inspected SSL traffic using a trusted certificate-issuing sub-CA?*	Yes -- Full SSL decryption. UMGC does not currently have the PKI systems or certificates to decrypt and re-sign SSL traffic.
8	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.3.5 states: "Each firewall unit must allow for both proxy-based and flow-based methods of inspecting traffic flows". *If <a prospective proposer> were to implement a proxy-based solution, would the flow-based requirements be lessened or remain as-requested in addition to what is performed on the proxy system?*	It would remain as requested.
9	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.1 Hardware.	Requirement 2.1.3.6 states: "Each firewall unit must have Data Loss Prevention ("DLP") capabilities". *Are there specific DLP capabilities that are required?*	Data in motion/at rest. To be able to use the firewall to inspect files, and block as necessary in multiple network segments. Use e-mail filtering and encrpytion as a preventative strategy. Data loss prevention for web sites (WAF).
10	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.2 Technical Support and Software Licensing.	Requirement 2.2.3.2 states: "Each firewall unit must provide remote user VPN connections". *How many unique users are required?*	Each should be capable of supporting five thousand unique users.
11	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.2 Technical Support and Software Licensing.	Requirement 2.2.3.4 states: "Each firewall unit must provide anti-spam protection". *Is it required that the firewall be in the flow for email (both send and receive)?*	Yes, it is required. Anti-spam protection is required for inbound and outbound flow of traffic.

Question No.	RFP Section	Question	UMGC Response
12	Section III. Procurement Phases and Evaluation Process; Paragraph 3. HECVAT LITE	*Is <UMGC> willing to sign an NDA for the HECVAT Document? This document contains proprietary information about the manufacturer and an NDA is required before release.*	Yes, UMGC is amenable to signing a Non-Disclosure Agreement ("NDA") if it is required for receiving the HECVAT LITE questionnaire and will use the University's standard NDA form.
13	Appendix A-2 Bid/Proposal Affidavit	*Appendix A-2 - is this document to be filled out by the reseller or the manufacturer?*	Appendix A-2 at pages 20 - 24 of the RFP document should be completed by the Offeror (i.e. the firm that is submitting a proposal in response to the RFP).
14	Section II. Scope of Work	<If a> *proposed solution will require a management station for logging and policy configurations,* <should> *this proposed solution include a virtual management station or dedicated management appliance?*	The proposed solution may include either a virtual management station or dedicated management appliance. Both are acceptable.
15	Section II. Scope of Work	*Will each site be independent of the others and will site gateways be managed by local management appliance, or could each site be managed by a centralized manager?*	Both sites will be managed by a centralized manager because there are rules that will be shared between the 2 sites.
16	Section II. Scope of Work	*Does the management of the gateways need to be a physical appliance or could it be cloud-based?*	We will not need any gateway.
17	Section II. Scope of Work	*Are there any logging retention policies that are required to be adhered to?*	No defined policy, but retention to match current in-place solution.
18	Section II. Scope of Work	*Is the 25gb SSL inspection throughout an average or peak requirement?*	It is a requirement per firewall.
19	Section II. Scope of Work	*If SSL-capable hardware is required, is SSL Inspection in-scope for this engagement?*	Yes.
20	Section II. Scope of Work	*Is there an internet bandwidth requirement?*	There is no internet bandwidth requirement.
21	Section II. Scope of Work	*Are members of each cluster located in different locations or is the HA requirement for clustering in different locations to accomplish redundancy?*	The members of each cluster will be located in the same physical location.
22	Section II. Scope of Work; Paragraph 2. Firewall Solution Requirements; Sub-Paragraph 2.3 Professional Services for Initial Configuration and Implementation	<Requirement 2.3.1 lists configuration of> Remote User VPN and Site to Site VPN. Neither firewall specification presently has them in scope (they are listed as zero) <in requirement 2.3.2 of the Scope of Work>.	See the updated Scope of Work attached to Addendum 1 for modification to these requirements. UMGC will require 5 remote access VPN groups and 1 site-to-site VPN be added to the new firewalls.
23	Section II. Scope of Work	*How many profiles are need for each of the 2 HA pairs?*	If this is referring to remote VPN profiles, the requirement is 5 profiles per cluster.