SECTION II. SCOPE OF WORK
(updated 3/18/2021 and attached to Addendum 1)

1. Purpose/Description.

1.1. University of Maryland Global Campus ("UMGC" or "University") is seeking to purchase next generation firewall hardware, software and related support and services as further described below. The hardware purchase will be made immediately following award of a contract so that all hardware can be implemented and configured by UMGC's required date of June 30, 2021. UMGC anticipates the Professional Services will be mutually scheduled with the awarded vendor and performed remotely and as soon as possible at a pace that ensures transition and change management do not interrupt the University's operations. Similarly, UMGC anticipates training will be mutually scheduled with the awarded vendor and performed remotely and as soon as possible at a pace that aligns with the configuration and migration of the University's current firewalls to the new firewalls.

2. Firewall Solution Requirements.

2.1. Hardware.

2.1.1. Four (4) firewalls to be configured in high-availability pairs in two (2) separate locations.

2.1.2. Each firewall unit must provide the following:

2.1.2.1. Firewall throughput of 56 Gbps to 240 Gbps
2.1.2.2. Threat prevention throughput of at least 23 Gbps
2.1.2.3. IPSEC VPN throughput of at least 13 Gbps
2.1.2.4. Maximum sessions of at least 50 M
2.1.2.5. Support for 20 to 24 10 Gig SFP+ interfaces
2.1.2.6. Redundant (dual) power supplies

2.1.3. Capabilities.

2.1.3.1. 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.
2.1.3.2. Must provide for real-time malware scanning of traffic.
2.1.3.3. Must provide URL traffic filtering capabilities.
2.1.3.4. Must be able to cluster HA pairs of firewalls across geographically distributed data centers.
2.1.3.5. Must allow for both proxy-based and flow-based methods of inspecting traffic flows.

2.1.3.6. Must have Data Loss Prevention ("DLP") capabilities including, but not limited to, data in motion/at rest; the ability to use the firewall to inspect files, and block as necessary in multiple network segments; to use e-mail filtering and encryption as a preventative strategy; and data loss prevention for web sites ("Web Application Firewall").

2.2. **Technical Support and Software Licensing.**

2.2.1. Provide manufacturer 24x7x365 dial-in support for all features with an initial response time of one hour or less.

2.2.2. Provide a Return Merchandise Authorization ("RMA") for defective/failed equipment within 24 hours.

2.2.3. Each firewall must provide the following software features:

2.2.3.1. General firewall software features
2.2.3.2. Remote user VPN connections
2.2.3.3. Site-to-site VPN (IPsec)
2.2.3.4. Anti-Spam protection
2.2.3.5. Web Filtering protection
2.2.3.6. Advanced malware protection
2.2.3.7. Intrusion Prevention System (IPS)

2.3. Professional Services for Initial Configuration and Implementation.

2.3.1. Configure four (4) firewalls in two (2) different locations, including:

2.3.1.1. System settings
2.3.1.2. System Logging
2.3.1.3. High Availability
2.3.1.4. Dynamic Routing
2.3.1.5. Remote User VPN
2.3.1.6. Site-to-Site VPN
2.3.1.7. Anti-Spam protection
2.3.1.8. Web Filtering Protection
2.3.1.9. Malware Protection
2.3.1.10. Advanced Malware Protection
2.3.1.11. Intrusion Prevention System (IPS)
2.3.1.12. Dynamic access policy

2.3.2. Migrate existing rules from UMGC's current Palo Alto 5050 firewall devices and add new rules* to the new firewalls. *New rules are highlighted below:

2.3.2.1. **Site 1**

- 3 physical interfaces per firewall

- ~2300 addresses
- ~162 address groups
- ~986 services
- ~42 service groups
- ~189 NATs
- ~125 security groups
- 1 site-to-site (this is a new rule, not an existing rule to be migrated)
- 5 remote access VPN groups (this is a new rule, not an existing rule to be migrated)
- ~37 static routes
- ~20 pre-rules
- ~300 post-rules
- ~2 default rules

2.3.2.2. **Site 2**

- 3 physical interfaces and 3 sub-interfaces per firewall
- ~409 addresses
- ~42 address groups
- ~126 services
- ~15 service groups
- 2 NATs
- ~64 security groups
- 1 site-to-site (this is a new rule, not an existing rule to be migrated)
- 5 remote access VPN groups (this is a new rule, not an existing rule to be migrated)
- ~15 static routes
- ~15 pre-rules
- ~50 post-rules
- ~2 default rules

2.3.2.3. Provide support during the cutover and immediate prioritized continual support for a period of two weeks after. Assume that UMGC will stagger the cutover to span one day for each location and occur one week apart, with all installation/configuration completed on or before 6/30/2021.

2.3.2.4. Provide a full knowledge transfer of firewall configuration and rules to the University technical staff.

2.3.2.5. Provide initial installation of hardware onsite at UMGC's locations. Some configuration services may be performed remotely offsite.

2.4. <u>Training.</u>

2.4.1. Provide remote, offsite comprehensive instructor-led firewall training for five (5) users.

2.4.2. Provide remote, offsite comprehensive instructor-led security feature-related (anti-spam, web filtering, malware protection, IPS) training for five (5) users.

2.5. <u>Higher Education Community Vendor Assessment Toolkit Lite ("HECVAT LITE").</u>

2.5.1. A qualifying score of "C" or better is required of the awarded reseller and manufacturer for this RFP.

END OF SECTION II: SCOPE OF WORK