**Instructions:** Answer in this Word document each of the questions. If attachments are needed to expand upon the narrative response, reference the question number in the attachment. Insert your company’s name in the footer where designated [*INSERT NAME of COMPANY]*

1. **Technical Questions**

Please respond to the following questions. Each question should be individually addressed.

* 1. Describe how your proposed architecture supports network segmentation to accommodate UA's different policy domains across various academic, student, research, administrative, and third-party units on the campus (e.g., administrative campus network computing vs. secure research enclaves for NIST 800-171 compliance vs. student residential Wi-Fi-centric commodity internet vs. UA Athletics large scale fan-facing wireless services). Please describe how this architecture can scale to support further segmentation of additional domains in the future and detail any scaling limits or constraints.
	2. How does your proposed architecture support identity-based networking to provision users and devices in appropriate segments with the necessary policies, access controls, and least privilege best practices?
	3. How does your proposed architecture support transitioning users or devices between policy domains or segments when they have requirements to participate in multiple policy domains or segments?
	4. Describe how your proposed network architecture integrates core firewalls that deploy, enforce, and manage policies across the various network segments.
	5. Describe your approach to data center networking and support for features such as microsegmentation, application centric policies, and orchestration of applications across traditional, cloud-native, and hybrid IT infrastructure (e.g., enterprise integration with cloud infrastructures).
	6. How does your proposed architecture automate or orchestrate deployment of network device configurations across approximately 20,000 routers, switches, and wireless access points?
	7. Describe how your proposed automation and orchestration capabilities will reduce UA staff time associated with managing the network and avoid growth in staff as the network expands.
	8. Describe your proposed network management and monitoring system(s).
	9. How does your proposed architecture support a model of network management and monitoring that enables role-based access control (e.g., enablement of differentiated access control for various distributed technical roles across campus academic, research, administrative, and third-party units)?
	10. Describe how your architecture supports integration with information security tools (e.g., SIEM, IDS, NAC, SASE), including descriptions of APIs supporting these integrations.
	11. Describe your capabilities to provide professional services support for development of the existing Azure Sentinel SIEM system, including identifying and aggregating additional telemetry data and log sources, and developing additional queries, dashboards, and reports in the SIEM system. Alternatively, recommend an alternative SIEM platform, articulate the value of migrating to the alternative SIEM, and describe your capabilities to provide professional services support to migrate operations to the new SIEM with complete aggregation of log/telemetry data, and development of recommended queries, dashboards, and reports on the new SIEM system.
	12. Describe your capabilities to deploy a network tapping and aggregation infrastructure to support security monitoring of east-west traffic flows of particular interest to UA (e.g. the Science DMZ environment).
	13. Describe how your architecture can support a migration over time from a premise-based secure remote access infrastructure (e.g., leveraging firewalls and/or vpn concentrator appliances) to a cloud-based secure access service edge (SASE) deployment.
	14. Describe reference customers where you have implemented solutions of similar size and duration of effort.
1. **Non-Technical Questions**

Please respond to the following questions. Each question should be individually addressed.

* 1. Based on your understanding of the network goals, technical questions, and technical requirements in Attachment I, describe your definition of the Next Generation Network, your approach to achieving the NGN, and how features of your proposed solution can improve UA’s delivery of network services.
	2. Describe your general approach to implanting the NGN including priorities, stages, and expected timing. Additionally describe the issues UA may face in transitioning from the current architecture to the next generation network in at least the following areas:
		1. WiFi
		2. Wired access
		3. Network management
		4. Licensing
		5. Security posture
		6. Research environment
		7. Other
	3. How is your solution optimized for UA to achieve a more secure future while providing a best-in-class user experience?
	4. What are the mechanisms for controlling pricing and achieving lowest total cost of ownership over the term of the relationship?
	5. What is your vision over the next five years?
	6. What do you think the market will look like in five years?
	7. What do you see as the role of 5G in supporting NGN?
	8. How will your solution enable UA to manage the network with fewer people or lower cost FTE? What training programs do you offer to enable UA network staff to effectively manage your proposed architecture?
	9. Provide sample SLAs that describe varying severity levels and access to engineering level staff in terms of timelines and escalation processes.
	10. What position in your company would be our executive point of contact?
	11. Confirm what is being proposed is not near or at the end of its production cycle?
	12. For the products proposed in your solution, identify the recommended refresh cycles and projected end of life cycle for all items.
	13. For the products proposed in your solution, identify by product where the components are sourced. Confirm how changes to your manufacturing processes and component sourcing are communicated to your customers.
	14. For the products proposed in your solution, identify by product where the product is assembled.
	15. Describe the checks undertaken to ensure your products are ISO compliant and do not introduce back door risks.
	16. The University cannot use any components manufactured by Huawei.  Confirm that in your proposed solution there are not any components or sub-components manufactured by Huawei or any other supplier restricted by the United States or the **state of Arkansas.**