INDIANA UNIVERSITY

PURCHASING DEPARTMENT

Request for Proposal:

RFP-TEC-1703-2025

For

Border Firewall Appliances

Indiana University

University Information Technology Services

Final Response due no later than
5:00pm (Eastern Time) on 3/28/2025

Issued by:
Rachel Beall
IT Purchasing Category Manager
Indiana University
2709 E 10th Street
Bloomington, Indiana 47408
Issued: 1/10/2025

Section A: Table of Contents – 2

Section B - Purpose

Indiana University (IU) is requesting proposals from firms interested in providing enterprise class network border firewall appliances and security solutions. The intent of this Request for Proposal (RFP) and the ensuing process is to provide companies with the information, requirements, and specifications necessary for the preparation of a professional and comprehensive proposal. Specific terms and conditions are outlined.

Selection of the successful company (Contractor) will be based upon:

- Ability to meet technical specifications and statement of needs
- Total cost of ownership
- References
- Value Add
- Acceptance of terms and conditions

These criteria have been listed in order of importance.

As used within this RFP, "Participant" shall refer to those companies receiving and responding to this RFP. "Contractor" shall refer to the successful Participant of the process. "University" shall refer to Indiana University.

If the Participant will not be selling directly to the University, it is the Participant's responsibility to choose one reseller with whom they will partner on this project.

Section C - Background

Founded in 1820, Indiana University is a public, multi-campus, 4 billion dollar educational institution with over 90,000 undergraduate and graduate students. All 50 states, Washington, D.C., three U.S. territories and over 150 foreign countries are represented. In addition to the student population, IU has over 21,000 faculty and staff supporting the educational mission of the institution.

IU spans the state with eight campuses. For more general information about the institution, please visit the institution's home page at https://www.iu.edu/ and the Institutional Research and Reporting site at https://uirr.iu.edu/.

The University Information Technology Services department (UITS) is charged with the mission of creating, implementing, and maintaining a network infrastructure to support scholarship throughout the University system. UITS manages this environment to facilitate the highest quality computing, voice and data infrastructure for research, teaching, learning and those administrative functions supporting the academic mission. Further efforts enhance the University's other missions of providing access to higher education for all citizens of the State of Indiana and to augmenting the economic development of Indiana.

UITS manages the network infrastructure for the IU campus core network infrastructure across the state of Indiana, the IU data centers in Indianapolis and Bloomington, and over 430 campus buildings across the state. With such broad responsibilities, UITS evaluates and deploys scalable enterprise class solutions that have a proven record of performance within peer institutions.

IU funds lifecycle refresh cycles for all critical network equipment. Network infrastructure components proposed for this solution must be best of breed in reliability and performance, but, at the same time, represent product innovation and price performance ratios to allow for highly scalable and resilient deployments.

Section D - Proposal Instructions and Conditions

D1 All questions and inquiries regarding this document should be submitted via the Jaggaer supplier portal. If you experience issues, you may contact Purchasing Category Manager, Rachel Beall, directly at rabeall@iu.edu. EXCEPT FOR CASES AUTHORIZED IN WRITING BY RACHEL BEALL, DURING THE DURATION OF THIS RFP PROCESS, THROUGH SELECTION AND NOTIFICATION, ANY COMMUNICATION BY PARTICIPANTS WITH INDIANA UNIVERSITY STAFF OTHER THAN RACHEL BEALL MAY RESULT IN IMMEDIATE REJECTION OF THAT PARTICIPANT. Questions regarding this RFP should be submitted through the Q&A Board within the Jaggaer supplier portal as they occur. Questions asked after the deadline shown in the schedule in Section E will not be answered

D2 Proposals (responses) should be submitted via the Jaggaer supplier portal. The responses must be received by the due date/time stated in Section E. Fax or Telephone Proposals will not be accepted.

D3 The University reserves the right to reject any or all proposals, and particularly any proposals not containing complete data requested. The University reserves the right to waive any irregularity in any proposal received. Proposal should be submitted initially on the participant's most favorable terms.

D4 The University will not pay for any information requested herein, nor is it liable for any costs incurred by the participant in responding to this request. All proposals submitted become the property of the University; they will not be returned and may be subject to the Freedom of Information Act.

D5 Participants may withdraw their proposals prior to the closing time. Proposals received after the time set for receipt will not be considered. The proposal constitutes an offer from the participant, which shall remain open and irrevocable for a period of 90 days.

D6 After the RFP closing time, proposals will be opened and reviewed at the convenience of the Purchasing team. There is no public opening.

D7 The University reserves the right to accept the proposal that appears to be in the best interests of Indiana University and to negotiate a contract with that participant using the proposal submitted as a basis.

D8 Any information released either verbally or in writing prior to the issuance of this request shall be deemed preliminary and not binding upon the University in any manner.

D9 If requested, participants must submit audited financial statements for the past two (2) years (or equivalent data) in order to demonstrate financial capability to provide the required services.

D10 Participants may be invited to come to Indiana University to provide a presentation about their submission at their own expense.

D11 The University will not enter into any agreement or execute any contract or affix signature to any document from a participant whose terms, written or verbal, require the University to waive all conditions or requirements negotiated, provided for in this document, our purchase order, or by mutual consent. Any document containing a clause or clauses that serve to supersede all other documents attached to this transaction may be rejected.

D12 Notwithstanding any other provision of this Request for Proposal, the University expressly reserves the right to:

1. Conduct discussions with any or all participants for the purpose of clarification of proposals;
2. Waive, or decline to waive, any insignificant defect or informality in any proposal or proposal procedures;
3. Accept, reject, or negotiate the terms of any proposal, or any parts thereof, for the purpose of obtaining the best and final offer;
4. Reissue a Request for Proposal;
5. Select the finalist(s) based on the University's analysis and evaluation of proposals submitted. The University reserves the right to request presentations of proposals if the University feels further information is appropriate to the decision-making process;
6. Negotiate with any or all the participant's representatives for the purpose of obtaining best and final offers. However, proposals will be evaluated on the assumption that the proposed costs/revenues are your most favorable.

D13 The University reserves the right to use any and all concepts presented in any reply to obtain the most beneficial and effective path to achieving the desired goals. Selection or rejection of submittals shall not affect this right.

D14 By virtue of submittal, the participant is attesting that all requirements, terms, and conditions in Section G have been read and understood. Unless the responding participant expressly and specifically provides otherwise in its written proposal, the proposal received in response to this Request for Proposal shall automatically be

deemed to include the responding participant's agreement to all terms and conditions of the RFP.

D15 Your response to this Solicitation constitutes an offer to do business with Indiana University under (at a minimum) the terms, conditions and pricing collectively gathered by this Solicitation process. In the event a contract is awarded, the University, at its option, may incorporate all or parts of your response in that contract. Any or all answers and information contained within your proposal shall become part of the final agreement between you and the University.

D16 All proposals or offers must be signed by a duly appointed officer or agent of your company.

D17 Unless judged a trade-secret, no part of your offer or proposal can be guaranteed proprietary or confidential. As required by the Indiana Open Records law, I.C. 5-14- et seq., submittals may become public information once a contract has been completed.

D18 Proposals responding to this Solicitation shall not be tied to any potential or future arrangements.

Section E - Schedule of Events

Following is the detailed schedule of events for this RFP. The University reserves the right to modify the schedule below.

	ACTIVITY	DATE
E1	Request for Proposal issued.	1/10/2025
E2	Participants' questions concerning the proposal must be received no later than 5:00 pm Eastern Time, in accordance with Section D1. An email response or status of response will be provided within 24 hours. If the information is related to substantive content of the RFP, then clarifications will be sent to all known participants of the RFP.	2/14/2025
E3	Proposals due by 5:00 pm Eastern Time, in accordance with Section D2.	3/28/2025
E4	Selection of vendor no later than	6/20/2025
E5	Delivery of equipment to begin, on or before	9/26/2025

Section F - Statement of Needs

Objectives

Indiana University (IU) is seeking to expand its network border protection mechanisms through the acquisition and implementation of new border firewall appliances and associated security services.

F1 Implement New Network Border Firewall Appliances

Design and implement new border firewall appliances expanding on the capabilities for real-time inspection and mitigation of malicious traffic, application-level policy enforcement, and advanced threat protection features using Next Generation Firewall feature sets and machine learning.

F2 Scope of Work

F2.1 **Proposal**

The selected Contractor must propose border firewall hardware, software, and related pricing, which meets the objectives and criteria defined in section F and technical requirements in section G.

Support and licensing pricing for 5 years for all components, including software and hardware should be included.

F2.2 **Training**

The selected Contractor must provide training for up to 15 University personnel. The training can be on-site at IU or delivered remotely. This training shall include instruction on the operating system, configuration, and troubleshooting of the equipment which is pertinent to the University's intended use of the equipment. Due to the scope of the project, training is a critical component to ensure the engineering staff can effectively expand and support the environment.

Describe in detail the training curriculum that will be offered to the University, the location of the training, and associated costs if any. It would be preferred for training to occur before or around the delivery of solution components.

F2.3 **Technical Support**

The selected Contractor must provide technical support from the equipment manufacturer on the proposed solution for a period of 5 years. Any hardware or software not covered under a lifetime warranty should include 5 years (60

months) of support, including software updates and next-business day hardware replacement.

Any support must include online access to software upgrades, online access to the manufacturer's knowledge base, online initiation of technical support cases, phone-based initiation of technical support cases, and initial response from a technical support engineer within two hours of initiating a technical support case, and next-business-day replacement of failed hardware.

F2.4 **Equipment Delivery**

Equipment should arrive on or before 9/26/2025.

F2.5 **Mitigation of Risk**

With a vast and complex networking environment, the Participant should describe how operational risk and downtime will be avoided during a phased deployment of network border security appliances and services.

F2.6 **Value Add**

Please describe any additional services that you would like to include at no cost to the University such as but not limited to the items listed below:

- Direct access to Tier 3 engineers for on-going support throughout the hardware life cycle.
- Tier 3 engineer availability on site for initial implementation.
- Ongoing training offerings for proposed solutions beyond the initial deployment year.

Section G - Proposal Response

The Participant's response to this proposal should include answers to the following series of questions. So that the RFP team can easily follow the questions and responses, please ensure that the question is stated immediately before the response. In addition to point-by-point responses, you may include descriptive literature if you refer to specific contents. In reviewing the proposals, university personnel will not search through general literature.

When a question is asked, answer the specific question and supply any supportive detail. Any deviation from this format and sequence may result in the proposal being immediately rejected.

While responses should address all solicitation items, it is important to note that we also encourage and will consider any creative ideas for functional improvements or cost savings related to this transaction that may not be suggested in this document. Functional, technical, and economic solutions beyond the confines of this solicitation may also be considered.

The responses should address all solicitation items. However, the University reserves the right to consider other ideas and solutions, or only a restricted subset of the configuration discussed in this document.

All optional arrangements should be described and priced separately.

G1 All proposal responses must include:

G1.1 The name, address, phone and fax number, and email address for the duly authorized agent submitting the proposal.

G1.2 Full description of company, including experience, qualifications and organizational chart.

G1.3 Documentation of any intent to partner with a reseller for any part or the whole of the services offered in response to this RFP.

G1.6 Copies of all documents that could become a part of a final Agreement arising from this process. A legal review of the Participant's proposed Agreement terms will be part of the criteria in evaluating the Participant's offer.

G1.7 The Participant must provide five reference customers. A minimum of two references must be from higher educational institutions of 25,000 students or greater within the United States using the proposed equipment in a similar manner to IU. However, three of these references are strongly desired.

G2 Pricing:

G2.1 Provide a proposal that includes the following:

- All hardware described in Section F, including associated support and licensing for 5 years,
- All necessary related components described in Section F., such as power-supplies, fan trays, transceivers, line cards, brackets, etc.
- Any additional software for monitoring, measuring, and troubleshooting the proposed border security infrastructure including associated support and licensing for 5 years.
- All pricing should be provided in line-item detail format

G2.2 Provide the cost, if any, for any training offerings.

G2.3 Please indicate if proposed Value Add items in Section F2.6 will be at no cost. Otherwise, please indicate line-item pricing for optional services.

G2.4 Specify any ongoing and protected, flat percentage (%) discount from manufacturer's list price for future purchases, including equipment not specified in the Participant's response. The discount structure should be firm for a minimum of five years, with an option to renew for an additional 5 years. Contractor must agree that the discount will be increased for University, if Contractor increases discounts generally to its customers above the offered discount to University, for the relevant goods and services. Contractor must agree list pricing shall not increase except as part of a non-targeted, across-the-board pricing increase by the Contractor, applicable to its customers generally, for the relevant goods or services. The selected Contractor will give IU at least 60 days' advance notice of any increase in the list pricing it charges to IU under the pricing agreement. Such an increase shall not exceed CPI or 3% each year of the term, whichever is lower.

G3 Provide point-by-point responses in Section F, describing in detail your company's capability of meeting the stated objectives and needs, while meeting the technical requirements beginning in Section G7.

G4 Describe in detail similar deployments your company has executed in the past 3-5 years.

G5 Describe in detail similar deployments your company has executed in the past 3-5 years for an institution of higher education within the United States.

G6 Describe your methodology for providing requested services, how you would organize your team and the IU team, and how you would ensure you deliver a quality product that meets expectations.

G7 All proposed solutions must offer components which support the following list of features. Please simply affirm or deny that your proposed solution meets the following requirements by notating each item with "accept," "deny," or "variance." Please explain any variances in your product. The Participant cannot answer "accept," if the feature is not currently available in the proposed hardware running current general availability (production) release software. If a feature is not in production software at the time of the RFP submission, the Participant must choose "deny" or "variance." If a feature not in production software is described under a "variance," it must be noted the feature is not currently available.

G7.1 Hardware, Performance, and Connectivity Requirements

(1) The border firewall proposal should include two dedicated firewall appliances capable of operating as a highly resilient HA pair (network architecture defined in Appendix A).
(2) The border firewall appliance pair should operate in a highly redundant fashion, such that a failure of one appliance does not impact campus connectivity or overall performance. The remaining appliance should be able to support all functionality requirements at full line rate.
(3) High availability of the border firewall appliance pair should not rely on any external layered service such as a load balancer.
(4) All border firewall appliances should be dedicated physical hardware (not virtual appliances).
(5) Each border firewall appliance must support a minimum of 100 Virtual Systems.
(6) Each border firewall appliance must support native 400Gb interfaces and connectivity for all feature sets or services included in the RFP response.
(7) Each border firewall appliance must support the complete outline of connectivity requirements defined in Appendix A.

G7.2 Firewall Feature Requirements

(1) The product must allow policy decisions to permit or deny traffic based on advanced protocol, application, and port information. For example, it should allow

for restricting traffic from specific applications like RDP or SSH in addition to traditional port and protocol-based filtering.

(2) The product must provide virtualization integration of firewall features, including micro-segmentation per machine and per groups of machines.

(3) The product must support the ability to apply policy decisions to allow or restrict traffic based on user identity, including both specific individuals and groups such as faculty, staff, students, and other organizational roles. This ensures that traffic control and management policies align with each user group's unique access requirements and security needs.

(4) The product must support the ability to restrict or permit the types of files transmitted to or from a protected network.

(5) The product must provide the ability to perform session-level network traffic inspection across all 65,535 network ports.

(6) The product must support real-time alert logging for blocked or allowed traffic.

(7) The product must support the ability to analyze and detect malicious files.

(8) The product must support SSL termination and decryption for inspection.

(9) The product must support the ability to detect and prevent data exfiltration.

(10) The product must support connection timeout values per protocol or port.

(11) The product must provide threat intelligence service features, including target industry categorization

(12) The product must apply threat intelligence to mitigate threats.

(13) The product must support the integration of third-party threat intelligence feeds.

(14) The product must support aggregation of threat intelligence from multiple sources and cross-correlate for accuracy.

(15) The product must support third-party integrations and can trigger automated actions for blocking, isolating, or quarantining devices into mitigation networks upon detection of threats. This feature should utilize standard communication protocols such as SOAP, REST, or equivalent APIs to interact seamlessly with external security tools, network devices, or mitigation systems. The integrations should enable rapid and automated responses to identified threats, isolating compromised devices, blocking suspicious traffic, or applying quarantine measures based on real-time threat intelligence. This ensures the containment of threats to prevent lateral movement or further compromise within the network while maintaining compatibility with various security ecosystems

(16) The product must support the ability to apply different security signatures selectively to distinct populations of machines or users, such as those used by faculty, staff, students, and administrative departments. This ensures each group receives tailored protection based on risk profile, usage patterns, and operational needs.

(17) The product must provide the ability to employ deep packet inspection for designated network segments.

(18) The product should support or integrate with honeypot technologies and/or have deception functionalities. These features would help lure attackers into decoy systems, enhance threat intelligence gathering, and delay or divert potential attacks from critical assets.

G7.3 Management Requirements

1. All communication between the border firewall appliance and the management software must be encrypted using industry-standard protocols.
2. The proposed management application must support the same feature set for IPv4 and IPv6 (i.e., feature parity). Any functional differences between IPv4 and IPv6 support must be individually noted in the variance explanation.
3. The proposed management application must provide a single point of configuration and management for the complete set of border firewall appliances included in the proposal.
4. Each border firewall appliance must include complete redundancy of management hardware modules operating as an active/passive pair.
5. The proposed management application and all border firewall appliances must support management role(s) and permission levels set via returned RADIUS Attribute-Value Pairs.
6. All border firewall appliances must support dedicated network management ports.
7. All border firewall appliances must support a serial management interface.
8. All border firewall appliances must support SNMPv2c and SNMPv3.
9. All border firewall appliances must support restricting management access via a locally defined access control list (or equivalent protection). This must apply to all management protocols supported on the proposed firewall (HTTPS, SNMP, SSH, REST, SOAP, etc.). All border firewall appliances must support the ability to restrict access by a combination of source IP and destination port.
10. All border firewall appliances must support RADIUS-based authentication for HTTPS (GUI), SSH and serial console users.
11. All border firewall appliances must represent the following information as objects that can be queried via SNMP
    1. Status of physical devices (chassis, fan trays, power supplies, line cards)
    2. Status of resources (CPU, memory, etc.).
    3. Status and statistics of internal processes.
    4. Status of physical interfaces.
    5. Traffic counters for physical interfaces.
12. All border firewall appliances and the management application must support failover to a locally defined user account if the RADIUS server is unreachable.
13. All border firewall appliances and the management application must support encryption of the RADIUS shared secret stored in the configuration file.
14. All border firewall appliances and the management application must support encryption of local user passwords stored in the configuration file.

15. All border firewall appliances and the management application should support sending logs to multiple centralized syslog servers.
16. All border firewall appliances and the management application must log usernames of authorized users to the syslog server at the time of login.
17. All border firewall appliances and the management application must log the username associated with a configuration change to the syslog server at the time the change is committed.
18. All border firewall appliances and the management application should support central time server synchronization using Network Time Protocol NTP V.4/PTP (RFC 5905).
19. The management application should support two-factor authentication for login using two successive RADIUS authentication queries to two different RADIUS servers. For example, a user should be authenticated with a username/password against one RADIUS server, and then the border firewall appliance should require and process a one-time password token against a second distinct RADIUS server.
20. All border firewall appliances should support a fully functional CLI management interface available through SSH and a serial port.
21. All border firewall appliances should report per-VLAN and per-interface traffic counters.
22. All border firewall appliances should support syslog over TCP.
23. The management application should support imports and exports of border firewall appliance configurations.
24. All border firewall appliances should support reporting the serial number and slot position of every field replaceable part.
25. All border firewall appliances and the management application should provide a rollback function to the last previously working configuration.
26. The product must support the use of applying, saving, and managing multiple configurations and multiple revisions.
27. The product must provide a layered approach to user, device, and policy management, including groups and global and local rules.
28. The product must support centralized reporting, creating reports based on individual firewall policies, customized groups, or across all firewalls.
29. The product must support granular access control of Application Programming Interfaces (APIs).
30. The product must support comprehensive policy tracking and management, including integration with ticketing systems for policy change requests, workflow management, approvals, and notifications. Additionally, the product must facilitate the entire lifecycle management of policies, ensuring that policies are regularly reviewed, updated, and optimized based on organizational needs, compliance requirements, and threat landscape changes. This includes automated reminders for policy reviews, audit trails for policy changes, and the ability to schedule periodic reviews and revalidations to maintain effectiveness and relevance.

31. The product must provide a robust, user-friendly Graphical User Interface (GUI) for reviewing alerts. The GUI should include the following capabilities. Please provide a specific answer for each of the line items for this section (G7.3.31.1, G7.3.31.2, etc.)
    1. **Search, Filter, and Query**: Allow analysts to easily search, filter, and query alerts to prioritize and investigate incidents quickly.
    2. **Alert Prioritization**: Enable the prioritization of alerts based on severity, impact, and other relevant criteria to streamline response efforts.
    3. **Export Functionality**: Provide the ability to export alerts for further analysis, reporting, or compliance purposes.
    4. **API Integration and Compensation**: The product should support API calls that complement and extend the GUI's capabilities, allowing automation and integration with other systems. APIs should compensate for any limitations in the GUI, enabling advanced queries, alert management, and workflow automation directly through API endpoints.
    5. **Accessibility and Ease of Use**: The GUI must be intuitive and accessible, designed to minimize the cognitive load on analysts and make work more efficient. It should be customizable to individual preferences to enhance usability.
    6. **Analyst-Centric Design**: Features should include configurable dashboards, quick actions, and clear visualizations that help analysts make faster, more informed decisions. The design should support multitasking and reduce manual effort through built-in shortcuts and automation options.
32. The product should provide policy management capabilities that support synchronization between on-premises and cloud environments. This functionality would enable consistent policy enforcement across hybrid environments, simplify management, and enhance overall security posture.

G7.4 Physical, Power, and Cooling Characteristics

(1) All border firewall appliances must support AC power supplies.

(2) All border firewall appliances must support power redundancy for AC power supplies, such that if any one power supply were to fail or lose power, the appliance would continue to function without impairment or degradation of service.

(3) All border firewall appliances must have hot-swappable power supplies, such that they are individually removable without impairing or degrading function.

(4) All border firewall appliances must have N+1 redundant fan modules, such that any single fan module can fail without impairing appliance function or requiring the appliance to shut down.

(5) All border firewall appliances must have hot-swappable fan modules, such that they are individually removable without impairing or degrading function.

G8 Each Participant must answer the following set of questions designed to help identify basic metrics, product scalability, and overall product suitability for enterprise deployments.

G8.1 Firewall Features

(1) Define the granularity of capabilities supported by your product at the application level (i.e. how application-aware your product is in reference to G7.2.1). Give specific examples in support of the overall scope and depth of capabilities stated.
(2) Specify how your product supports the ability to apply policy decisions to allow or restrict traffic based on user identity (as it relates to G7.2.3). Can it integrate with remote identity repositories? If so, specify which, and the mode(s) of authentication supported.
(3) Specify how your product integrates with other systems (as it relates to G7.2.15) to facilitate automated actions for blocking, isolating, virtual patching, of devices or network traffic. Define the modes of the integrations and any other tooling within your portfolio that can complement the security features offered by the product.
(4) Please provide comprehensive detail regarding the overall HA configuration for the proposed solution. Please document triggers for the high availability process, how traffic failover is handled both in a failure and recovery scenario, and any expected impact on production traffic or user experience. Highlight any differentiators in the proposed solution that make it a market leader in terms of overall stability and reliability in large-scale production deployments.

G8.2 Firewall Performance

(1) Please provide expected throughput maximums for the proposed solution when operating with complex application and identification rules enabled. Include information on how these configurations might impact performance, specifying the possible throughput rates under various load conditions. This data will help evaluate the firewall's performance under realistic, high-demand scenarios.
(2) Are there architectural limitations of the ASIC's on a per port basis that we should consider when selecting interfaces as standalone or in an LACP trunk ? If "yes" please provide interface to ASIC mapping details.

G8.3 Firewall Management

(1) Elaborate on any features or mechanisms included in support of appliance configuration management, including management and tracking of policies, configuration rollback (particularly in reference to G7.3.20 and G7.3.26).

(2) Specify inherent tools or mechanisms in the proposed solution to identify stale or outdated security policies with no recent traffic or activity.
(3) Specify inherent tools or mechanisms in the proposed solution to set expiration timelines or triggers for specific policy.
(4) Specify inherent tools or mechanisms in the proposed solution to stage new policy or security services in test/dev environments before they are advanced from test/dev to production environments.
(5) Elaborate on automation capabilities using Ansible or other common network automation frameworks.

G8.4 Hardware Maintenance and Service

(1) Specify the proposed border firewall appliance release date(s).
(2) If it exists, specify the proposed border firewall appliance end-of-sales date(s).
(3) If it exists, specify the proposed border firewall appliance end-of-support date(s).
(4) Describe, in detail, your hardware support and replacement methodology in the event of a large-scale natural disaster or national incident. Specify any FEMA frameworks that are used as a reference architecture for your response process.

G8.5 Physical, Power, and Cooling Characteristics

(1) Describe any capabilities for power utilization monitoring and reporting within the proposed solution.
(2) Specify the height, in number of rack units, for the proposed devices.
(3) Specify the depth, in number of inches, for the proposed devices.
(4) Specify the width as suitable for 19" or 23" rack width.
(5) Specify mounting options for 2 or 4 post racks, front, rear, and/or mid.
(6) Specify the maximum power consumption of the proposed network hardware when fully populated.
(7) Specify the maximum BTU output of the proposed network hardware when fully populated.
(8) Specify the capabilities in the proposed hardware for hot insertion and removal of components such as modules/power supplies/fan trays. These tasks should not require a reboot of the hardware or create any disruption in the functionality of the hardware.
(9) Specify any capability of the proposed solution to perform predictive analysis of hardware to alert on potential issues prior to hardware failure.

G9 Each Participant is encouraged to list features that provide additional value or functionality not described above.

G10 Each Participant should provide electronic copies, or web access, to documentation for the proposed solution components.

G11 At the request of Indiana University, selected participants may be asked to perform Proof–of-Concept testing (PoC). While Indiana University can accommodate an onsite PoC, engineers may choose to travel on-site or request a remote-PoC if the participant is able to accommodate. Testing will be geared towards configuration, performance, and resiliency.

If a PoC is requested, participants will collaborate with engineers to formulate a PoC plan. Participants may also provide a PoC proposal with their response describing their capabilities to meet the requirements above. Indiana University reserves the right to add or remove test items. A copy of final configuration files from all tested switches should be provided in addition to relevant test results and metrics at the conclusion of the PoC.

G12 Participants may be asked to provide a two-year (24-month) product roadmap during the RFP process.

G13 If a Participant lists a feature or hardware that is not in production at the time of proposal submission, the Participant must describe how they will verify the feature is in production code or that hardware will be available no later than 6/20/2025. This verification must include notation of the added feature in software release notes and possible demonstration of the feature on the proposed equipment using production code. Hardware must be customer orderable on or before 6/20/2025. The Participant is responsible for any costs associated with feature verification.

G14 The submission must be signed by a legally authorized agent of the firm.