THE UNIVERSITY OF
SOUTHERN MISSISSIPPI

3 March 2026

Addendum 4 for RFP 26-26

This responds to questions submitted by potential respondents. The University's answers are shown in red.

Amber Floyd

Amber Floyd

Buyer, Procurement, and Contract Services

1. How many locations do you need supported as part of this project?
    a. The University operates a distributed campus environment with multiple academic, administrative, and residential facilities. Vendors should assume support for multiple locations typical of a public research university; however, specific site counts are not provided, and solutions should not require customization based on individual location characteristics.

2. How many total endpoints do you have?
    a. Specific endpoint counts are not provided. For proposal and pricing purposes, respondents should base their assumptions on an average active user population of approximately 9,500 (previous 30 day range is 7100 to 12000) users generating telemetry across endpoints, identity, email, and cloud services.

3. What are the OS versions for the 300 servers that need monitoring?
    a. Operating system versions for the approximately 300 servers requiring monitoring are generally not disclosed. Vendors can assume a 50/50 split between windows server and OEL.

4. Can you please list out what security solutions you are currently using from your Microsoft 365 A5 agreement? (examples- Defender, Sentinel, or Cloud Apps)
    a. Vendors should assume a comprehensive Microsoft 365 A5–comparable security posture and propose solutions that integrate broadly with Microsoft's security ecosystem without reliance on specific configurations being disclosed.

5. What solution are you currently using for Identity and Access Management?
    a. The University uses an enterprise-grade identity and access management platform with multi-factor authentication. Specific products or versions are not disclosed.

6. How many total IP addresses are part of the initial assessment requirements?
    a. Total internal and external IP address counts are not provided. Vendors should assume a large enterprise environment with numerous internal and external IPs, and should not assume that all internal IP addresses are reachable from a single location.

7. How many wireless networks do you have?
    a. The number of wireless networks is not disclosed. Vendors should assume multiple wireless networks supporting academic, administrative, and residential use cases.

8. Are you looking for the MSSP provider to also supply solutions or just monitor your existing solutions for each of the below requirements
    a. Monitor existing solutions.

9. What solutions are currently being used to perform the functions outlined in your initial assessment request?
    a. Specific solutions used for identity, email, endpoint, server, and cloud security are not disclosed. Vendors should assume the presence of industry-standard enterprise security controls consistent with a Microsoft 365 A5–level environment.

10. Are you using or looking to use an EDR/XDR Solution? If yes. What solution are you using? If No, What solution do you use at the endpoint?
    a. The University operates endpoint protection and detection capabilities consistent with enterprise best practices. Proposed solutions should support integration with MS Defender EDR/XDR technologies.

11. Do you currently perform Threat hunting as part of your security operations?
    a. The University performs security monitoring and investigation activities but does not disclose specific threat-hunting practices. Vendors should describe if their managed service includes threat hunting capabilities.

12. Do you currently have a SIEM? If so, which SIEM and what version?
    a. The University is currently onboarding new data sources to Sentinel.

13. What model and version # of Firewalls is being used? How many firewalls?
    a. Firewall models, versions, quantities, and event rates are not disclosed. Vendors should assume enterprise-grade perimeter and internal firewalls generating significant security telemetry and propose solutions that are vendor-agnostic.

14. Which email solution are you using? What version?
    a. Assume M365.

15. What solution is deployed to secure your email environment?
    a. Email security controls are in place consistent with enterprise best practices, but specific solutions, versions, and deployment models are not disclosed. Proposed solutions should integrate with common cloud-based email security architectures.

16. Are you using any IDS/IPS solutions? If yes, what is the solution, version and how many are deployed?
    a. The University does not disclose whether IDS/IPS solutions are deployed, nor their versions or quantities. Vendors should assume environments where network-based detection controls may exist.

17. Are you currently using a vulnerability management solution?
    a. Specific vulnerability management tools and versions are not disclosed. Vendors may describe how their solution supports or complements vulnerability identification and remediation prioritization.

18. Which cloud platforms are you using? (AWS?, AZURE?, Google (GCP)? Combination of or other?)
    a. Azure.

19. Which, type, version and how many Databases are used in the environment?
    a. Database types, versions, and quantities are not disclosed, nor is the use of database-specific protection tools. Vendors should assume the presence of enterprise databases supporting academic and administrative systems.

20. What is the current size and makeup of your security team?
    a. The size and structure of the University's internal security team are not disclosed. The managed service is intended to augment existing staff and provide 24x7 SOC capabilities.

21. Do you currently have an Incident and Response Retainer in case of an outbreak?
    a. The size and structure of the University's internal security team are not disclosed. The managed service is intended to augment existing staff and provide 24x7 SOC capabilities.

22. Do you use a ticketing system as part of your IR process? If yes, which ticketing system and version do you use?
    a. The University uses an enterprise IT service management and ticketing platform; however, specific products and versions are not disclosed, and direct integration is not required.

23. What business driver is causing the need for this service?
    a. The primary drivers for this service are to enhance the University's ability to prevent, detect, investigate, and respond to cybersecurity threats; improve visibility and coordination across a complex enterprise environment; support governance and risk management objectives; and strengthen overall cybersecurity resilience while minimizing operational disruption.
24. Would you mind to receive the service from another country in the same time zone, but not from USA?
    a. Proposals may include services in other countries. This will be carefully considered. However, vendors must disclose location of services within their proposal.

25. Would it be possible to have a technical clarification call for scope/ requirement understanding before delivering the proposal?
    a. No . The University will not conduct technical clarification calls prior to proposal submission. All necessary scope, requirements, assumptions, and environmental details are fully documented in the RFP, and vendors are expected to base their proposals solely on the information provided.

26. Would you allow redlines for the contract terms?
    a. Yes. The University will allow vendors to submit proposed redlines to the contract terms as part of their proposal. All requested exceptions or modifications must be clearly identified and submitted in writing for review. Acceptance of any redlined terms is not guaranteed, and the University reserves the right to accept, reject, or negotiate proposed changes based on institutional, legal, and procurement requirements.

27. Can you please describe your institutional governance and risk management
    a. The University's cybersecurity program aligns with generally recognized higher-education and public-sector best practices. Proposed solutions should support governance, risk management, and compliance activities aligned with commonly adopted frameworks (e.g., risk-based, maturity-oriented models). Vendors may describe how their solution supports such frameworks within their proposal.

28. Is it correct to assume that all licensing on MS Defender is covered by USM or is it expected for Provider to provide licensing?
    a. All licensing for MS Defender is provided by USM.

29. Is it possible to change current MS Defender for another technology in a MSSP model? This means that licensing will not be USM owned.
    a. No.

30. Is MS Defender stack already deployed or has a full deployment to be considered? If so, what is the % of current implementation?
    a. MS Defender is fully deployed. Currently, USM is working to onboard new data sources to sentinel.

31. Is it correct to assume that MS Defender components to be managed are:
    - Microsoft Defender for Endpoint
    - Microsoft Defender for Identity
    - Microsoft Defender for Cloud

    Is MS Sentinel included in your licencing?

    Is there any other MS Defender module considered to be managed?

    a. Yes. All of the Defender XDR ecosystem is in scope.

32. Do you expect vender to use a service desk of USM? How would the access be provided to it? Or can the ticket handling and follow up be provided differently?

    a. Vendor can use their on portal. All incident response actions must be pre-arranged prior to service start date.

33. In the understanding USM has MS A5 licensing and is entitled to use MS Sentinel as a SIEM, is it correct to assume that provider must use MS Sentinel to manage alerts?

    a. Generally yes. However, this is a service offering over the top of USM's security stack. The current model does not support shipping logs to a vendor tenant.

34. In case the solution could be not MS Defender, is it correct to assume that data collection will be narrowed to endpoint data and identity data for threat detections?

    a. See response to question 31.

35. How often shall penetration testing be performed?

    a. Annually

36. Of the 9500 users, what is the student to faculty ratio? Or is that 9500 faculty.

    a. The University does not require vendors to further differentiate licensing or pricing by user type. Proposed solutions should be capable of monitoring and protecting a mixed population of faculty, staff, and student users generating telemetry across identity, endpoint, email, and network-based controls.

37. Do the students and faculty share the same O365 domain?

    a. Yes

38. What are the retention requirements?

    a. 90 days

39. Being a cybersecurity company, we have Non-Disclosure Agreements in place with our customers. Can we provide the requested references once downselected?

    a. The University recognizes that some vendors operate under customer non-disclosure agreements. Vendors may describe relevant higher-education or enterprise experience in a generalized manner within the proposal. The University reserves the right to request customer references or conduct reference checks during later stages of the evaluation or prior to award.

40. Please distinguish between faculty/staff count and student counts.

    a. For proposal and pricing purposes, respondents should base their submissions on an average active user population of approximately 9,500 total users, as stated in the RFP. This population includes faculty, staff, and students.

    b. The University does not require vendors to further differentiate licensing or pricing by user type. Proposed solutions should be capable of monitoring and protecting a mixed population of faculty, staff, and student users generating telemetry across identity, endpoint, email, and network-based controls.

    c. The last 30 day range for active users has been approximately 7100 to 12000 active users within M365.

41. Are students fully segmented on their own network(s)?

    a. The University operates a segmented enterprise network environment that supports academic, administrative, and residential use cases. Vendors should assume the presence of multiple network segments and varying trust zones and propose solutions capable of operating effectively in such environments. Additional network architecture details are not provided as part of this RFP.

42. Please provide physical and virtual server counts, hypervisors, and public clouds in use.

    a. For proposal and pricing purposes, respondents must assume approximately 300 servers requiring security monitoring, inclusive of physical and virtual instances, as stated in the RFP.

    b. The University operates a largely virtualized on prem environment. Specific hypervisor platforms, versions, and cloud service providers are not provided. Proposed solutions must be primarily focused on the M365 Defender Ecosystem.

43. Please list locations with direct internet access and corresponding aggregate internet speed.

   a. The University operates a distributed campus environment with centralized and localized internet connectivity. Vendors should assume enterprise-grade bandwidth and multiple ingress/egress points typical of a public research university. Specific site-level connectivity details are not provided. Solutions should not require customization based on individual building connectivity characteristics.

44. Please provide number of subnets and subnet classes.

   a. Subnet counts and addressing schemes are not provided. Proposed solutions must support environments with numerous subnets and varying IP address classes commonly found in large enterprise and higher-education networks.

45. Please list current security software/tools in place that are potential sources for monitoring and telemetry.

   a. The University currently operates a comprehensive enterprise security stack comparable to Microsoft 365 A5–level licensing, as stated in the RFP. Vendors should assume the presence of commonly deployed enterprise controls, including but not limited to:

      i. Identity and access management with MFA
      ii. Endpoint protection and EDR
      iii. Network firewalls and VPN services
      iv. Email and collaboration security
      v. Cloud and SaaS security telemetry

   b. Specific vendor products and configurations are not disclosed. Proposed solutions must demonstrate broad integration capability with industry-standard security technologies.

46. Please list any IT service management tools in use.

   a. The University utilizes an enterprise IT service management (ITSM) platform. Specific products are not disclosed as integration with the ITSM is not required.

47. Please provide mailbox counts and licensing for Microsoft 365 and Google Workspace.

    a. For proposal purposes, respondents should assume:

        i. A mixed population of faculty, staff, and student users utilizing cloud-based productivity and collaboration platforms

        ii. An enterprise licensing model comparable to Microsoft 365 A5

        iii. A single-tenant enterprise environment

    Specific mailbox counts, license SKUs, and platform distribution are not provided. Solutions must support integration with major SaaS identity, email, and collaboration platforms used in higher-education environments utilizing the Microsoft ecosystem.

48. Please specify log retention requirements longer than 90 days.

    a. At this time, the University does not mandate a log retention period beyond 90 days. Vendors may propose configurable retention options and associated cost impacts as part of their solution.

49. Please list cybersecurity frameworks being referenced or measured.

    a. The University's cybersecurity program aligns with generally recognized higher-education and public-sector best practices. Proposed solutions should support governance, risk management, and compliance activities aligned with commonly adopted frameworks (e.g., risk-based, maturity-oriented models). Vendors may describe how their solution supports such frameworks within their proposal.

50. What are the opening times on Monday 9th of your room 214?

    a. 2:00 PM CST

51. Is it mandatory to provide a sealed envelope or would the electronic copy be sufficient to participate in the tender?

    a. An electronic response submitted through MAGIC is acceptable. These instructions may be found on the current bids webpage and in the RFP.

52. You want to have a 45 days payment term. Could you agree to a 30 natural days payment term?

    a. Net 45

53. Do you plan upfront service payment with contract signature? Or is the payment after the 1st year for the 1st time? Would you accept monthly payments?

    a. All additional contract negotiations shall be discussed upon award.

54. For vendors that provide unlimited users and unlimited data ingestion, can you provide an asset count for devices (servers and workstations) that reside in your primary Active Directory instance?

    a. Prices should be based on average active user counts rather than enabled user accounts within the environment. That approximate number has been provided and is listed in the RFP that you attached. Our last 30 days has ranged between approximately 7100 to 12000 active users within M365.

55. Regarding the scope and desired outcomes for the Penetration Testing services, can USM provide additional details on what is expected?

    a. Penetration testing is not the primary area of concern. Up to 10 IP addresses and one comprehensive website test must be included.