



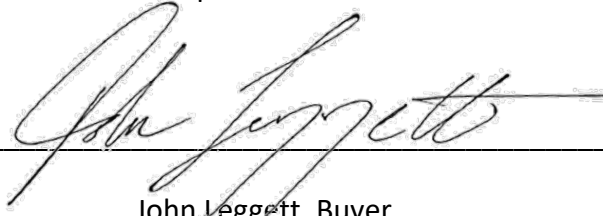
THE UNIVERSITY OF SOUTHERN MISSISSIPPI

May 17th, 2022

Addendum 1 to RFP 22-45 Managed Security Services/Managed Detection Response.

This addendum provides answers to questions submitted by prospective bidders. The

answers to the questions below are in red.



John Leggett, Buyer

1. **Are there any air gap networks?** *We have air-gapped hosts, and they are not in scope.*
2. **What are the 3500 IoT devices and OS listed in Appendix C?** *Most are VoIP handsets, but can also be some PLC controllers, IP cameras, and environmental controllers (IoT spec is OPTIONAL)*
3. **Do you want to include Incident Response as a part of MDR? (IR retainer is optional add-on)** *No, not beyond SOC like services.*
4. **Will the University consider a five-year contract, billed annually?** *Yes.*
5. **Does the University still want to use its existing SIEM and endpoint security technologies? Or do you want to replace those?** *We do not want to use our current SIEM. It says in the RFP we are replacing it. We are open to replacing end point security, but it's not required*
6. **(A) Are you looking for us to completely manage like writing firewalls rules or making changes in Active Directory?** *No.* **(B) Or do you want traffic to be ingested by a tool and simply correlate the data from various sources?** *Yes, but preferably with MDR.*
7. **Do you need software updates to be completed?** *No.*
8. **Do you need patching?** *No.*
9. **Do you want to own the technology or have someone own it and manage it for you?** *We would prefer to NOT to buy a device or incur a capital cost. It's acceptable if the solution requires it, just so long as USM isn't responsible for any management or maintenance tasks of on-premise devices (per the RFP).*

PROCUREMENT SERVICES

118 College Drive #5003 • Hattiesburg, MS • 39406-0001

Hattiesburg • Long Beach • Ocean Springs • Biloxi • John C. Stennis Space Center



THE UNIVERSITY OF
SOUTHERN MISSISSIPPI
1848

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

10. Line 28 Appendix C "Software agents should provide capability for full auditing of all actions taken on the system" : What specific actions are you looking for?

This is a "preferred" feature request: we would like to see a solution that will capture events related to file operations by system, users, and processes (file writes, file reads, memory reads, delete modify etc.), as well as systems operations by processes and users (spawning of processes, termination of processes, user privilege elevation, user management, etc).

11. Line 45 Appendix C "Syslog/Syslog-ng" : What applications is the syslog ingesting data from?

Various. Mostly, system messages from the OS. Our firewalls and network devices also use syslog.

12. Line 69 Appendix C "Service provider must maintain University data exclusively within the geographic US" : Does this pertain to metadata?

If a breach of the metadata would pose a risk to the university or an individual, then yes. If a required feature isn't implemented at all, it may not be a dealbreaker (per the directions documented in Appendix C).

13. Line 70 Appendix C "The solution must provide integration with AD and MS Azure SSO for authentication" : Does the administrator management interface require SSO?

Yes – It's 'required' but if the solution can't do it, an alternate or partially implemented feature is acceptable. If a required feature isn't implemented at all, it may not be a dealbreaker (per the directions documented in Appendix C).

14. Line 143 Appendix C "Solution should provide integrity controls" : Can you please define integrity controls?

In this case: file integrity monitoring is desired, if possible (but it's not required...)

15. Is USM hosting their active directory onsite? Or Azure?

We have a kind of a hybrid thing going on, we sync our AD on prem with Azure AD – I believe we've been slowly migrating all authentication to Azure AD, but we don't think we are there yet.

PROCUREMENT SERVICES

118 College Drive #5003 • Hattiesburg, MS • 39406-0001

Hattiesburg • Long Beach • Ocean Springs • Biloxi • John C. Stennis Space Center