Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

16 Central Street
Bangor, ME 04401-5106

Main: 207-973-3200
TDD/TDY: 207-973-3262
www.maine.edu

REQUEST FOR PROPOSALS #41-13
Network Data Center Review
University of Maine System
ADDENDUM #1

The University of Maine

University of Maine at Augusta

University of Maine at Farmington

University of Maine at Fort Kent

University of Maine at Machias

University of Maine at Presque Isle

University of Southern Maine

This addendum reflects responses to vendor inquiries:

Q1. What are the make and model of the Primary Routers in Orono and Portland?

A1. Orono: Cisco Catalyst 6509, Supervisor 720 3BXL; Portland: Cisco 7609, RSP 720 3CXL

Q2. Can you specify the number of virtual servers and the number of physical servers?

A2. There are roughly 400 virtual machines on 20+ VM host systems, and roughly 100 physical servers. See the original RFP for details on the hosts:

Section 1.4 Scope: There are roughly 500 hosts in the Orono data center and 50 hosts in the Portland data center. The Orono data center has 34 VLANs and the Portland data center has 5 VLANs. Both IPv4 and IPv6 are utilized in the data centers. Please see Attachment A for more information on the data center network architecture.

Q3. If available, can you provided sanitized diagrams of the core and infrastructure environments in Portland and Orono?

A3. This information will be provided to the awardee.

Q4. Can you provide sanitized configuration files of the two Primary Routers?

A4. This information will be provided to the awardee.

Q5. Are the third-party systems housed in the data centers expected to be within scope of the review?

A5. No, third party systems are not in scope, but maintaining the support of the third party systems is.

Q6. Often physical security controls are key to protecting critical systems (especially in shared data centers), is evaluation of these controls within scope?

A6. No.

Paragraph 1.6.1 Documentation of the Oron data center to be used as a starting point for common understanding. Sounds like they need documentation, but not clear on WHAT kind of documentation. I am assuming network mapping (doable via network discovery scans plus router configuration review), but they may also want documentation on what equipment is in what rack in the data center along with physical wiring diagrams.

Q7. It is not clear how many networks are in play, nor how large the networks are.

A7. See section 1.4 of the original document.

Section 1.4 Scope: There are roughly 500 hosts in the Orono data center and 50 hosts in the Portland data center. The Orono data center has 34 VLANs and the Portland data center has 5 VLANs. Both IPv4 and IPv6 are utilized in the data centers. Please see Attachment A for more information on the data center network architecture.

Q8. We don't know what routers and switches they have in place, making configuration review or route tracing challenging/impossible.

A8. This information will be provided to the awardee. The infrastructure is by and large Cisco-centric with 6500 series routers and Nexus series switches.

Q9. We don't know what kind of routing protocols are in use in the network, making it hard to estimate how much time would be needed to perform route tracing.

A9. EIGRP is used for Layer 3 between routers. The majority of networks at each facility terminate on the primary router.

Q10. Is the University expectin a physical datacenter diagram? If so, how big is the Orono data center? Square footage? Number of racks?

A10. No, we are not expecting a physical diagram.

Q11. Is the University expecting a physical wiring diagram? If so is it just for Ethernet, or will it include fiber, coax, or POTS lines? Will we have to trace serial cables or terminals?

A11. No, we are not expecting a wiring diagram.

Reference 1.6.2 Recommendations for security architecture at the network, storage and system levels. I am guessing that this one is where we detail a new recommended secure environment, while the next section details how to migrate from the old environment to the new one.

Q12. In order to provide security recommendations for the network, we'll need configurations for every routing device in the network, a way to perform a configuration review, a way to model it in the network as a whole, and more fine grained UMS input on their desired security objectives.

A12. Configuration information for relevant devices will be provided to the awardee.

Q13. In order to provide security recommendations for storage (assuming NAS or Fibre Channel), we'll need to understand what systems need access to each storage device, and that's going to require a good understanding of the applications in use in the environment. If the University doesn't already have this mapped out, this can be a considerable amount of discovery time, let alone the architectural design work necessary to ensure access to the storage devices is secure.

A13. A point-in-time map of storage assets can be provided to the awardee. Roughly, two filers 300 virtual hosts rely on one or both of the filers for operation.

Q14. In order to provide security recommendations for the endpoint systems (assuming servers for the most part rather than student desktops), we can perform credentialed scans of the target IPs. We'll need to know what OSes are in play in the environment we'll be assessing, as well as how many IPs are utilizing those OSes. Depending on the extent and rigor of the recommendations that the University is asking for, we may also be asked about hardening, AV, anti-malware, HIDs, etc...

A14. Credentialed scanning will not be an option in this engagement. Uncredentialed scanning will be permitted. Information regarding the host configuration can be provided as needed.

Reference 1.6.3 Recommendations for implementation of the architecture to achieve improved security.

Q15. Without knowing the extent of change required to bring the datacenter into alignment with the recommendations from 1.6.2, this is a question mark.

A15. To provide a solution for 1.6.3, the previous steps will need to be completed.

Q16. To what extent is the University seeking documentation/recommendations for third-party (non-University related) systems specified in paragraph 1.3?

A16. Third party systems are not in scope, but maintaining the support of the third party systems is. As an example, individual security controls for the third party systems isn't expected, but support in how we can better deliver service would be.

Q17. Are we safe to assume that our documentation/recommendations will be limited to the two data centers? In other words, we won't be including endpoints and closet switching around campus?

A17. Yes.

Q18. The time frames states: Consulting work should begin no later than July 25, 2013 with an estimated conclusion of around September 25, 2013. What is the outside limit for the completion date for the project?

A18. In reality, the completion date isn't a hard and fast date. It is a guideline. That being said, the timeframe in which the project can start and conclude will be factored into the final decision.

Q19. Does UMS have a current network diagram? If yes, can UMS share it with prospective bidders?

A19. This information will be provided to the awardee.

Q20. Does UMS have a current inventory of system assets? If yes, can UMS share it with prospective bidders?

A20. There is not a current inventory of assets. Host discovery of assets in the data center is expected to be within scope of this engagement.

Q21. Does UMS have a current, documented risk management program and risk analysis of system assets? If yes, would UMS be willing to share it with prospective bidders?

A21. Yes. The risk management program is outlined on our website at:
http://www.maine.edu/system/infosecurity/RiskAssessment.html

Note that most hosts do not have a current risk assessment completed on them. The data on the hosts with assessments performed can be shared with the awardee.

Q22. Does UMS have an approved, mid-to-long range strategic technology plan? If yes, can UMS share it with prospective bidders?

A22. There is no strategic plan that is relevant to the work to be done in the data center. We are seeking guidance that would seek out position toward an overall strategic plan.

Q23. Does UMS have a documented production change management process/policy in place? If yes, can UMS share it with prospective bidders?

A23. Uniform change management procedures have not been implemented.

Q24. Has UMS contracted for an independent security review, vulnerability analysis, or penetration test of its infrastructure? If yes, when was the last audit conducted?

A24. The PCI network has had a formal penetration test completed this year. Most of the assets in the data center had not.

Q25. How many IT staff are employed by UMS? How many staff are considered network architects or network engineers?

A25. There are roughly 200 IT staff and about 10 employees in a network architect or engineering role.

Q26. Does UMS contract for third-party systems support?

A26. No.

Q27. How many "tenants" are co-located at UMS data centers?

A27. This number is not known and we are hoping to have a better understanding after the review.

Q28. How many administrative domains are running?

A28. This number is not known and we are hoping to have a better understanding after the review.

Q29. What hardware and operating systems are mission-critical applications running on?

A29. The hardware is a mixture of virtualized assets and rack mounted systems. Operating systems are varied, Cisco IOS, Windows Servers, and various distributions of Linux operating systems.

Q30. What host-based firewalls are running?

A30. Windows firewall and IPtables primarily.

Q31. How many routers are running in the network? What are the make and model of the routers?

A31. Orono: Cisco Catalyst 6509, Supervisor 720 3BXL; Portland: Cisco 7609, RSP 720 3CXL

Q32. How many switches are running in the network? What are the make and model of the switches?

A32. (Limited to the scope of the two datacenter environments) Orono: Cisco Nexus 5596UP environment with 12 48-port fabric extenders. Portland: One 6509 (primary) and a pair of 4948 switches.

Q33. Have intrusion detection/prevention systems (IDS/IPS) been implemented? If yes, what systems are used?

A33. Yes, intrusion detection systems are in place. They are based off of Snort.

Q34. Have any network connection and performance management/monitoring tools been implemented? If yes, what tools are used?

A34. Yes. NMIS is used system-wide for monitoring of network devices. We also maintain a perfSONAR server for performance testing. iperf is used extensively for throughput testing.

Q35. Has UMS budgeted for this architecture study? If yes, can the budget amount be shared?

A35. Yes, this is a budgeted project. No, the budget can not be shared.

Q36. What are the expected formats and what information is expected to be documented in the starting point documentation deliverable?

A36. Expected formats are a standard report for a management level audience. Supporting raw data can be delivered in any standard output format (XML, .nessus, pcap, .nmap, etc).

Q37. Does the University currently have accurate documentation such as system inventories and network maps to support the initial documentation or does the vendor need to perform discovery activities?

A37. We are expecting the vendor to perform discovery activities.

Q38. Does the university currently have network security technologies such as IDS, IPS, etc?

A38. Yes, we currently have intrusion detection sensors in place.

Hal Wells
University of Maine System
Assistant Director of Strategic Procurement

June 14, 2013