



16 Central Street
Bangor, ME 04401-5106

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

**REQUEST FOR PROPOSALS #13-13
IT Forensic and PCI Investigation Services
University of Maine System
ADDENDUM #1**

In response to vendor inquiries, the University offers the following:

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

- Q1. Are any of the University systems subject to acquisition by the selected vendor maintained by third parties or hosting providers?**
- A1. The majority of University of Maine System systems that are subject to forensics under this RFP are maintained by the University; however the University may elect to enter into hosting agreements with third parties. The University wants bidders to state, in their proposal, whether the bidder can provide forensic investigation of third party hosted systems and if there is any cost or process variance.**
- Q2. Are University systems commonly deployed with logging software, anti-malware, and host based firewalls that might aid in the investigation process?**
- A2. University systems are commonly deployed with anti-malware, host based firewalls, and native OS logging, however there is no guarantee that a system that has been compromised has all these features employed.**
- Q3. Does the University have a preference as to the location of analysis following system acquisition?**
- A3. No, provided proper protections are met.**
- Q4. Is the "in scope" University systems inventory limited to the listed operating systems, i.e. Windows, OS X, Linux, Android, and iOS?**
- A4. Generally yes, however Solaris is also utilized.**
- Q5. Can the University provide a high level overview of Maine's IT systems inventory?**
- A5. No, our infrastructure is too dynamic.**
- Q6. Does the University have a consolidated log management system or utilize a third party to achieve log consolidation?**
- A6. Not at this time.**

- Q7. Does the University have an internal secure data sharing mechanism to be use during forensic investigations?
- A7. Not for everyday business use, but we can deploy a secure sharing mechanism as needed.
- Q8. Can you provide locations where forensic investigators are most likely to be deployed?
- A8. Forensic investigation could occur at any one of our seven campuses the prioritization listed below is based upon the number of systems each campus houses from largest to smallest. It is less likely that an event could occur at an off-site location.

<u>CAMPUS</u>	<u>CITY</u>
UMaine	Orono
USM	Portland
UMA	Augusta
UMF	Farmington
UMPI	Presque Isle
UMFK	Fort Kent
UMM	Machias

- Q9. The RFP requests vendors agree to define their response times within 4 hours for remote support and within 2 days for onsite work. Is it the intention of the RFP to execute a contract with a chosen vendor or are you looking for a vendor to commit to time objectives without execution of a contract?
- a. Our firm can only define time objectives if there is a retainer contract in place with monetary compensation provided during the duration of the contract. Essentially, we offer a block of consulting hours to be used within a specified timeframe but cannot commit to response times outside of executed contracts.
- b. An additional statement within the RFP indicates performance of an awarded project would determine if subsequent projects would be awarded during the contract. This leans towards the University simply gathering a list of potential vendors to execute ad-hoc contracts versus a blanket contract for a specified duration of three years as indicated within the RFP.
- A9. The University does not desire to enter into a retainer contract. We understand that vendors can only define time objectives if a retainer contract is in place, however with that being said, your response should show what you can offer without a retainer and what you can offer with a retainer.
- Q10. Will you consider responses with a greater defined response time? Our firm typically defines response times as 8 hours for remote support and 72 hours for onsite support.
- A10. The University will consider responses with a greater defined response time. The RFP states the 4 hour and 2 day response times as examples as it was our intent to describe what we felt to be reasonable times, however we are not restricting any vendor to the times specified.



 Hal Wells
 University of Maine System
 Assistant Director of Strategic Procurement

February 1, 2013