



DATE: January 9, 2012

TO: All Prospective Proposers

FROM: Janet Foster  
AVP Procurement Services  
240-684-5141

RE: RFP 90986 – Managed Security Services  
Addendum #3 dated 01/09/2012

The following amends the above referenced RFP documents. Receipt of this addendum is to be acknowledged by completing the enclosed "Acknowledgement of Receipt of Addenda Form" and including it in the Technical Proposal.

The due date for questions has been extended to 10 AM on Wednesday January 11, 2012.

The due date and time for the **Technical and Price Proposals** is **Tuesday, January 17, 2012 on or before 4:00 p.m.**

Proposals **must** be delivered to:

Janet Foster  
University Center UC 310  
4716 Pontiac Street  
College Park, MD

Late proposals cannot be accepted. Proposals are to be delivered to the University's Procurement Office, University of Maryland University College, Procurement Office, Room UC-310, 4716 Pontiac Street, College Park, MD 20740. The University recommends against use of mail or delivery services which will not guarantee delivery directly to Suite 310. Directions to the UMUC Procurement Office can be found at the website [http://www.umuc.edu/visitors/locations/uc\\_building.cfm](http://www.umuc.edu/visitors/locations/uc_building.cfm).

**Questions from Potential Proposing Firms  
Managed Security Services  
Addendum #3 dated 01/09/2012**

1. **Question:** Which applications are you looking to protect? Please provide name of application and quantity of each. Please include the number SQL, Oracle or Exchange instances to be monitored. **Response:** All
2. **Question:** For desktop monitoring, what is/are the monitoring objective(s)? Basic system activity monitoring only or a full deployment which can include file integrity management and usb activity monitoring? **Response:** Full deployment to include of the above mentioned and the monitoring of any illegal communication traffic.
3. **Question:** What are the existing vulnerability scanning capabilities if any? **Response:** In the process of implementing Rapid 7.
4. **Question:** Do you want us to collect netflow data? **Response:** Yes
5. **Question:** What is your NAC or other endpoint solution if any? **Response:** In the process of rolling out Cisco NAC
6. **Question:** How many Data-Center and Remote locations is your network distributed?  
**Response:** We have 5 data centers, 3 US, 1 Germany & 1 Japan
7. **Question:** Please provide approximate Average and Peak EPS (Events per Second) of current Log volume generated by each device count in provided list of network components?  
**Response:** We are unable to provide this information
8. **Question:** Does your network infrastructure currently aggregate all logs to a central location or more than 1 location? **Response:** More than 1 location
9. **Question:** For NIDS/NIPS, what is the bandwidth of network connections from the internet each of your ISP network demarcation points? **Response:** 1 Gbps
10. **Question:** Please provide a high level Network Topology Map to include geographic location, of network components to be monitored/managed. **Response:** See attached document.
11. **Question:** For the purpose of sizing, please provide model numbers and physical chassis configuration (modules, interfaces) of each Firewall in list of network components? What are your current Network Management Platforms assigned to Manage and Monitor your firewall platforms? **Response:** See Exhibit A.
12. **Question:** For the purpose of sizing, please provide model numbers and physical chassis configuration (modules, interfaces) of each router/switch/Wireless AP in list of network

components? What are your current Network Management Platforms assigned to Manage and Monitor your router/switch/Wireless AP platforms? **Response:**

- **Cisco Catalyst – Layer 3**
  - 6500
  - 4500
  - 3750
- **Cisco Routers**
  - 4600
  - 2800
  - 3800
- **Cisco Aironet Wireless**
  - WCS
  - WLC -4400
  - WLC -5500
  - Ap-3500

**13. Question:** For the purpose of sizing, please provide model number and physical chassis configuration (modules, interfaces) of Juniper SSL VPN Gateway in list of network components? What is your current Network Management Platforms assigned to Manage and Monitor your SSL Gateway platform?

**Response:**

All Cisco ASAs are managed using Cisco CSM as well as standalone  
All Juniper IDPs are managed and monitored using Juniper NSM  
All Cisco PIX devices are managed standalone  
All Cisco IPS devices are managed using Cisco IDM and standalone  
All Juniper SSL VPN devices are managed standalone  
All Checkpoint firewalls are managed using Checkpoint Smartcenter  
All Juniper SRX firewalls are managed standalone using Jweb and CLI

**14. Question:** Can you share the release version of the CheckPoint IP690s? **Response:** Nokia IP690

**15. Question:** What type of endpoint AV client is deployed? Are the feeds from the clients going to a management console, and would it be acceptable to pull data from the manager versus the client? **Response:** McAfee EPO 4.0 (In the process of implementing 4.6) Client VirusScan Enterprise & AntiSpyware Enterprise 8.70i. Yes, we wouldn't be opposed to pulling data from the console.

**ACKNOWLEDGEMENT OF RECEIPT OF ADDENDA FORM**

**RFP NO.:** 90986

**TECHNICAL PROPOSAL DUE DATE:** Tuesday, January 17, 2012 at 4 PM

**RFP FOR:** Managed Security Services

**NAME OF PROPOSER:** \_\_\_\_\_

**ACKNOWLEDGEMENT OF RECEIPT OF ADDENDA**

The undersigned, hereby acknowledges the receipt of the following addenda:

Addendum No. 1 dated 01/03/2012

Addendum No. 2 dated 01/04/2012

Addendum No. 3 dated 01/09/2012

Addendum No. \_\_\_\_\_ dated \_\_\_\_\_

Addendum No. \_\_\_\_\_ dated \_\_\_\_\_

As stated in the RFP documents, this form is included in our Technical Proposal.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Name Printed

\_\_\_\_\_  
Title

## Exhibit A

Sr. No.	Device	Location	# of Interfaces	Platform
1	ICC TLS Firewall ASA 5550	Adelphi	4 in use	ASA 5550 code 8.2.1
2	ICC-DC-Replication Fw (ASA-5510)	Adelphi	4 in use	ASA5585 code 8.2.1
3	Checkpoint FW 1	Adelphi	7 in use	Nokia IP690
4	Checkpoint FW 2	Adelphi	7 in use	Nokia IP690
5	ICC-PIX515E (Backup TLS to PG)	Adelphi	2 in use	PIX 8.0.4
6	Lab-Marroit-ASA 5510	Adelphi	5 in use	
7	Lab-Marroit-IPS	Adelphi	1	IPS-SSM module 7.4
6	ISP Firewall ASA 5550	Largo	3	ASA 8.2.1
7	ISP Firewall ASA 5550 (Standby)	Largo	3	ASA 8.2.1
8	TLS Firewall ASA 5520	Largo	1	ASA 8.2.1
9	TLS IPS ASA 5520	Largo		IPS SSM 7.4
10	IDSMP ISP - 1	Largo		IDSMP2 7.4
11	IDSMP ISP - 2	Largo		IDSMP2 7.4
12	Juniper SRX (Active)	Largo	8 in use	JUNOS [10.4R3.4]
13	Juniper SRX (Standby)	Largo	8 in use	JUNOS [10.4R3.4]
39	Faculty Media Lab ASA5510	Largo	3 in use	ASA 8.2.1
40	IPS for the Faculty Lab ASA	Largo	1	IPS SSM 7.4
14	PIX-535 firewall	PG1	2	PIX 8.0.4
16	PG-PIX-515E (backup TLS)	PG1	2	PIX 8.0.4
17	ASA 5510	Dorsey	3	ASA 8.2.1
18	IPS	Dorsey	1	IPS SSM module 7.4
19	PIX 515E	Travis CA	1	PIX 8.0.4
20	ASA 5510	Andrews	2	ASA 8.2.1
21	IPS	Andrews	1	IPS SSM module 7.4
22	ASA 5540 (active)	Europe	3	ASA 8.2.1
23	ASA 5540 (standby)	Europe	3	ASA 8.2.1
24	IPS - (active)	Europe	1	IPS SSM module 7.4
25	IPS - (standby)	Europe	1	IPS SSM module 7.4

### Exhibit A (Continued)

Sr. No.	Device	Location	# of Interfaces	Platform
26	ASA 5520 (active)	Asia	3	ASA 8.2.1
27	ASA 5520 (standby)	Asia	3	ASA 8.2.1
28	IPS - (active)	Asia	1	IPS SSM module 7.4
29	IPS - (standby)	Asia	1	IPS SSM module 7.4
30	ASA-5510	Bolling	2	ASA 8.3
31	IPS	Bolling	1	IPS SSM module 7.4
32	ASA-5510	Ft. Meade	2	ASA 8.3
33	IPS	Ft. Meade	1	IPS SSM module 7.4
34	ASA -5540- ISP(active)	DR	3	ASA 8.0.4
35	ASA -5540- ISP(standby)	DR	3	ASA 8.0.4
36	IPS (active)	DR	1	IPS SSM module 7.4
37	IPS (standby)	DR	1	IPS SSM module 7.4
38	ASA5510--REPLICATION	DR	3	ASA 8.2.1
39	SSL VPN Adelphi	Adelph	2	Juniper SA 4000
40	SSL VPN DR -Pair	DR	2	Juniper SA 4000