RFP ADDENDUM
February 18, 2014

ADDENDUM NO. 1 TO ALL OFFERORS:

Reference – Request for Proposals:	RFP #14-34
Commodity Code/to Furnish Goods or Service:	83845, 20854, 92014, 91829; POLICE CAD & RMS SYSTEMS SERVICES
Dated:	February 7, 2014
For Delivery to:	University of Mary Washington, Commonwealth of Virginia
Proposal Due Date:	**February 27, 2014; 3:00 PM**

This addendum consists of four (4) pages.

ADDENDUM #1

I. Clarifications to RFP:
   A. Addition to section X. Special Terms and Conditions:
   E-VERIFY PROGRAM: EFFECTIVE 12/1/13. Pursuant to Code of Virginia, §2.2-4308.2., any employer with more than an average of 50 employees for the previous 12 months entering into a contract in excess of $50,000 with any agency of the Commonwealth to perform work or provide services pursuant to such contract shall register and participate in the E-Verify program to verify information and work authorization of its newly hired employees performing work pursuant to such public contract. Any such employer who fails to comply with these provisions shall be debarred from contracting with any agency of the Commonwealth for a period up to one year. Such debarment shall cease upon the employer's registration and participation in the E-Verify program. If requested, the employer shall present a copy of their Maintain Company page from E-Verify to prove that they are enrolled in E-Verify.
   B. RFP Response Requirements including Electronic Media (Section V. A. 4 & V.B.9):
   "In order to be considered for selection, Offerors must submit a complete response to the RFP. If proposal is submitted in person, one (1) original (paper) and an electronic media version (DVD, CD or flash drive) of each proposal must be submitted to the University in the quantity requested." *Please submit 5 electronic media versions (i.e., 5 DVDS, CDs or Flash Drives.)* ***No faxed or emailed submissions will be accepted.***
   C. Referencing front page final deadline for acceptance of questions (emailed only): No questions will be accepted after 2:00 PM, 2/21/2014.

II. List of Mandatory Pre-Proposal Attendees (see attachment)

III. Q & A from Offerors:

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

A. Is the University currently operating in Fiscal Year 2014, which ends on June 30, 2014? Do funds for this FY need to only be encumbered by the end of June?
The University is currently operating in FY 2014, which ends June 30th. The acquisition of goods and services, receipt of invoice and full payment for the CAD/RMS Project all must occur by the final Accounts Payable cycle which occurs near the end of June. This is why the University's timeline is extremely tight.

B. Is the University's current data scheme for the existing product for the UMWPD server-based?
Yes.

C. Are there any images in the current files?
Yes, there are some photos.

D. Does the University have duplicate master names in the current configuration?
Yes.

E. How will information provided by Offerors in the submitted proposals be evaluated outside of the requirements forms?
It is assumed by the University that Offerors, in order to present the best-fitting package for the University, will provide additional information within their proposals outside of the requirements forms. This information will be taken into consideration in addition to the responses within the requirements forms; to arrive at a total score for the proposal based on the criteria indicated in the original RFP.

F. How many seats will be required for 24-7 Dispatch?
Two (2)

G. How many seats will be required for the future Mobile client module?
15

H. How many seats will be required for the RMS System?
A reasonable number would be five (5).

I. Are there travel rates per Commonwealth of Virginia (per diem) that must be honored?
Yes. Please review: http://adminfinance.umw.edu/ap/travel/per-diem-and-lodging-rates/

J. How many IBRs are recorded per year?
Approximately 750 – 800 emergency and non-emergency calls are recorded. The current system is not accurate and comingles the types of calls.

K. Will the cost of any hardware come out of the budgeted $100k set aside for this project?
Yes. If a physical server is purchased, the University will purchase it out of the project funding, based on the contractor's recommendations in conjunctions with University standards (per the RFP).

L. Is there Wi-Fi on campus?
Yes. It can be somewhat unreliable.

M. Are there floor plans (for each building) available?
Yes. There are floor plans for each campus building that will be available to the awarded contractor.

N. Are there 911 addresses for all buildings on campus?
No. Building names will be used for address locations.

O. Is there any GIS data available?
Yes, there is GIS data available in a limited sense. It can be shared with the awarded contractor.

P. If 911 is called from a campus line, will it go to the UMWPD dispatch?

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

No. If 911 is called from a campus phone, it will go to the City of Fredericksburg Police Department. The University emergency number is a 4-digit number from a campus phone and a regular number (10-digit) from an outside line.

Q. Does the University wish to be tied to 911?
No.

R. What is the most important functionality of the required system for UMW?
A robust RMS and CAD is the most important feature for the first contract year. Additional components will need to be budgeted for future contract years; after approval of cabinet level management and by the University's Board of Visitors.

S. Is there available funding for support of new systems (assuming RMS and CAD) for future years?
Yes.

T. What is UMW's vision for mobile data?
Mobile Data functionality is strictly a future desire that is currently unfunded; but, must be a readily available option should funding be secured within any given contract year.

U. How many dispatch positions do you need?
Two.

V. Page 4 – Item #1 -What is your current network configuration?
The University's network configuration is fairly standard for the industry:

a. *Ethernet*
b. *TCP/IP*
c. *DHCP/DNS*
d. *Microsoft AD*
e.

W. Page 7- Item E.1.d – What is the "UMW Network and Computer Use Policy" that must be followed?
Please see attachment.

X. Page 11, Item F.1. – What are the VA travel rates/ per diem?
Please review this link: http://adminfinance.umw.edu/ap/travel/per-diem-and-lodging-rates/

Y. Page 12 – please confirm that submission of 1 original hardcopy and 1 electronic media are sufficient—no other uploading of the proposal is required.
Please review Clarifications above for this information.

Z. It does not look like all of the listed attachments are numbered the same as the list. (We) just want to be sure we include in the proper sequence.
Attachment A: SCC Form
Attachment B: Small Business Subcontracting Plan
Attachment C: Interoperability Services Agreement
(ISA) Attachment D: SWaM Initiative Letter
Attachment E: SWaM Subcontracting Reporting Instructions
Attachment F: Project Pricing Form
Attachment G: - **Labeled as H** Computer Aided Dispatch (CAD) Requirements
Attachment H: **Labeled as I** Law Enforcement Records Management System (RMS) Requirements

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

Attachment I: **Labeled as J** Mobile Client and Mobile Field Reporting Requirements
Attachment J: **NOT Labeled – should this be G???** Standard UMW Contract Template

Please complete and return all required documents, regardless of sequence, preferably in one section, all together, within the proposal package.

AA. Also – the following is listed as Attachment I on the bottom says page 2 of 2… what does it go with? There is no Page 1 of 2?
The Attachment I page is the second page of the UMW Standard Contract/Master Agreement Template (page 1 of 2). This section (Attachment I) is where any mutually negotiated details of the contract would be listed; therefore, it is currently blank.

END OF ADDENDUM #1

Melva Kishpaugh, VCO
Asst. Director, Procurement Services
Phone: 540/654-1084

*Acknowledged receipt of RFP 14-34 Addendum #1 (and all addenda) should be acknowledged and included in the RFP submittal package:

_____ _____
SIGNATURE DATE

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

University of Mary Washington
Request for Proposals: RFP 14-34
UMWPD CAD & RMS SYSTEMS SERVICES
February 17, 2014; 2:00 PM

PLEASE PRINT LEGIBLY

NAME	COMPANY	PHONE #	FAX # / E-MAIL
MELVA KISHPAUGH - UMW		540/654-1084	mkishpau@umw.edu
DOUG EBBINK - ID NETWORKS		440-536-0084	debbink@idnetworks.com
JAY JOHNSON	FINFOR	205-902-1151	JAY.JOHNSON2@FINFOR.COM
JEFF LEWIS	DAPROSYSTEMS	888 377 4427	JEFFLEWIS@DAPROSYSTEMS.COM
Steve Libera	Southern Software	828-291-9147	slibera@southernsoftware.com
Lee Hoisington	Hyperion Inc.	703-981-1625	LHoisington@hyperioninc.com
David Ruesch	Hyperion Inc	703-848-8850 x3033 703-989-8814	druesch@hyperioninc.com
Mehrdad Negahban	beamSmart	202 573 8777	
Michael W Hall	UMW Police	540-654-1635	mhall2@umw.edu
Brad Sullivan	UMW Police	540-654-1638	bsulliv2@umw.Edu
Ruth Lovelace	UMW Em'l Safety	540-654-2096	RLOVELAC@UMW.EDU
Suzan Mastin	UMW - IT	540-654-5975	SMASTINC UMW.EDU

* - indicates a required field.

* **POLICY NAME:**	**Network and Computer Use Policy**
* **POLICY TYPE:**	Presidential Policy - University Administrative Policy
POLICY #:	E.4.4.
***STATUS:**	Active
***CONTACT OFFICE:**	Information Technologies
***OVERSIGHT EXECUTIVE:**	Chief Information Officer
***APPLIES TO:**	All Faculty, Staff, and Students
***PURPOSE:**	The UMW computer network consists of an institution-wide backbone, local area network, and many shared computers, as well as individual desktop computers and other computing devices. The various systems administrators work to ensure that network privileges are properly maintained for all University users. Users also must meet certain responsibilities and are subject to certain limitations. This policy outlines the requirements and responsibilities of users of the UMW computer systems and network and the consequences of non-compliance with this policy.
DEFINITIONS:	
***POLICY STATEMENT:**	Users of information technology resources at the University of Mary Washington must use them responsibly and within limitations. Users who fail to meet their responsibilities or who fail to operate within the limitations may have their network privileges suspended or revoked and may be subject to other disciplinary actions. Using University-owned computers, networks, or other information technology resources constitutes acknowledgment that the user understands and commits to compliance with the University's Network and Computer Use Policy and related policies and procedures. **PRIORITIES OF THE NETWORK** The UMW computer network and other information technology resources should be used, and will be maintained and administered, in accordance with the following priorities: • Highest and Primary: To support the education, research, and administrative purposes of the University of Mary Washington. • Medium and Secondary: To support other uses indirectly related to the University of Mary Washington's purposes with education or research benefits, including personal communications.

DISCLAIMER
The University of Mary Washington will investigate credible allegations of violations of the rules set forth below and will impose appropriate sanctions. However, the University assumes no responsibility for user conduct. Investigations of violations will follow the IT Security Incident Response Plan.

Users should be aware that there are many services on the Internet that they might find offensive or that involve risks. Users must accept responsibility for their own navigation of the Internet.

PRIVACY
The UMW computer network is owned and operated by the University of Mary Washington, an agency of the Commonwealth of Virginia. Faculty and staff must recognize that computer-generated documents (e.g., old e-mail) may be "public records," subject to provisions of Virginia's Freedom of Information statutes. Furthermore, all users must understand that electronic communications may not be secure and that during the course of ordinary management of information technology services, technical staff may inadvertently be exposed to the content of user files.

In specific and unusual circumstances, the content of user files may be examined under the direction of a system administrator of the system holding those files. This may be done only at the direction of the University President.

SAFETY
While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications in violation of this policy or state or federal law should bring them to the attention of the Department of Information Technologies and/or the University Police.

INTELLECTUAL FREEDOM
The network provides an open forum for the expression of ideas, including viewpoints that are strange, unorthodox, and unpopular. Opinions expressed there must be presented in a manner that is free of obscenity (as defined by Code of Virginia section 18.2-372), forgery, and other illegal forms of expression, which are not acceptable uses of the University's network and are in violation of University policy. In addition, expressions of opinion may not be represented as the views of the University of Mary Washington, and individual users are responsible and accountable for any material posted and transmitted on the network in violation of this or other University policies, or state or federal law.

USER RESPONSIBILITIES
Current employees (faculty and staff) and students, as well as employees who have retired from service at the University, are eligible to have computing accounts. In addition, some other parties, such as scholarly partners of faculty and contractors employed at the University, may be granted computing accounts for limited terms with appropriate sponsorship. To enjoy the privileges of computer use and network access, each user of University information technologies is expected to meet certain responsibilities and honor certain limitations. If a user is found to have knowingly violated either of these

	principles, his or her network access may be suspended. Depending on the seriousness of the violation, the user may also be subject to other University disciplinary actions, and violations of federal or state laws will result in referral to the appropriate legal authorities.
	
	The following list of responsibilities applies to the use of all University-owned computers and of the University's networks; additional responsibilities may be associated with specific networks, information technology services, and computers at the University.
	
	• Users must operate within the appropriate federal or state laws and University policies and must not engage in any conduct that presents a risk to the operating integrity of the systems and their accessibility to other users.
	• Users must abide by the terms of all software licensing agreements and copyright laws. Users must not make copies of or make available on the network copyrighted material, unless permitted by a license.
	• Users must not use the network resources of the University to gain or attempt to gain unauthorized access to remote computers, networks, or systems.
	• Users shall not engage in any activity that alters wired or wireless network connections, access points, topology, or physical wiring of university owned resources.
	• The use of University computer resources and networks is for legitimate academic or administrative purposes.
	• Users may not use University-owned computers or networks to access, produce, or distribute pornography in violation of the law.
	• Users will not divulge confidential or highly sensitive data to which they have access concerning faculty, staff, or students without explicit authorization.
	• Any network traffic exiting the University is subject not only to provisions of this policy, but also to the acceptable use policies of any network through which or into which it flows.
	• Users should notify the Division of Information Technologies IT Help Desk (654-2255 or it-abuse@umw.edu about violations of computer laws and policies, as well as about potential vulnerabilities in the security of its computer systems and networks.
	• Users are to respect the rights of other users, including their rights as set forth in other University policies for students, faculty, and staff; these rights include but are not limited to privacy, freedom from harassment, and freedom of expression.
	• Users may not place on any University-owned computer system any type of information or software that:
	  ○ infringes upon the rights of another person.
	  ○ gives unauthorized access to another computer account or system.
	• Users may not misrepresent themselves or their data on the network.
	• Users are responsible for the use of their accounts. No user may give anyone else access to his or her account, or use a UMW computer account assigned to another user. A user must not attempt to obtain a password for another user's computer account.

	• Users are responsible for the security of their passwords and for regularly changing passwords in accord with good practice and with the rules of the system in which the password is used. Users are responsible for making sure no one else knows their passwords. A user who suspects someone knows his or her password should change the password immediately (or contact Division of Information Technologies (654-2255) if he or she needs assistance in changing the password). • Users of personal computers are responsible for protecting their work by making regular backup copies of their work files and storing the copies in a safe location. They should set the frequency of backup based on their ability to recreate information added since the last backup. • Users must not attempt to monitor other users' data communications, nor read, copy, change, or delete other users' files or software, without permission of the owner(s). • Users must not attempt to circumvent data protection schemes and computer and network protections or exploit security loopholes. • Users must not deliberately perform acts that are wasteful of computing or network resources or that unfairly monopolize resources to the exclusion of others. • Users must not deliberately perform acts that will impair the operation of computing equipment, peripherals, other devices, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer. • Users must not run or install on any of the computer systems of the University, or give to another user, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This includes, but is not limited to, the classes of programs known as computer malware, viruses, Trojan horses, and worms. • Users may not use the University's computer systems or networks for solicitation of funds or for commercial purposes. This includes solicitations for charitable or community organizations. • Users may not use the University's networks to distribute chain letters. • Users must not illegally download or distribute, including via peer-to-peer file sharing, copyrighted material. This policy and related material supplement the existing policies in the Student Handbooks and the UMW Employee Handbook for Administrative/Professional Faculty, Classified and Wage Employees. These cover such acts as theft of computer services (including copyrighted computer programs), theft or mutilation of UMW property such as computer equipment, and the unacknowledged or unauthorized appropriation of another's computer program, or the results of that program, in whole or in part, for a computer-related exercise or assignment. Ultimately, any and all network conduct or misconduct is subject to the same policies that govern conduct in other University venues, and it is regulated and dealt with as described in the handbooks cited above.

	VIOLATIONS Violations or suspected violations of the policies and principles enumerated above should be reported promptly to the Division of Information Technologies at 654-2255 or it-abuse@umw.edu , or to the appropriate University department. **SANCTIONS** Responses for violation of this policy may include, but are not necessarily limited to, the following: • Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations. • Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty. • Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently or for a specified period of time. • Restitution for damages: requiring reimbursement for the costs of repair or replacement of computer-related material, equipment, hardware, software, data and/or facilities. In addition, such reimbursement shall include, but not necessarily be limited to, the cost of additional time spent by University employees due to the violation. Violators may be subject to criminal or civil penalties as they apply. The University considers any violation to be a serious offense in its efforts to preserve the privacy, data, and services of individuals and the University. In the case an investigation is begun related to policy and/or legal violations, the University's officials reserve the right to access, examine, intercept, monitor, and copy the files, network transmissions, and/or on-line sessions of any user. The University may choose to suspend a user's access to its resources in connection with investigation of (but not limited to) any of the following: • Violations or suspected violations of security and/or policies • Activities that may be contributing to poor computer performance • Computer malfunctions. The University's Office of Human Resources (as well as appropriate UMW or external law enforcement agencies) may be notified of the violation and provided with information and materials relating to the investigation and/or violation. In connection with investigations, files, data, or communications may be shared with the appropriate investigating officials. In general, the University will exercise discretion as far as is appropriate given the case.
PROCEDURES:	
* General	**NETWORK ADMINISTRATION**

Procedures for Implementation:	The Division of Information Technologies, working with the administrators of UMW computer systems and networks, has the responsibility to protect the rights of users, to enforce policies and procedures consistent with those rights, and to publicize those policies and procedures to their users. The department has the authority to control or refuse access to any user who violates these policies or threatens the rights of other users, and department officials will make reasonable efforts to notify users affected by decisions they have made. Questions or concerns regarding the use of the University's network, its computers, or other information technology facilities or services should be addressed to the Division of Information Technologies, 540-654-2255, or helpdesk@umw.edu.
* Process for Developing, Approving, and Amending Procedures:	As a result of the required annual review, the CIO or her/his designee will make appropriate changes to the policy and present them to the University President for approval. Additional amendments will be handled on a case by case basis at the discretion of the CIO.
* Publication and Communication:	The policy is on the UMW website and is covered in required annual security awareness training for all employees. Data Stewards and Data Security Contacts complete additional annual training. The policy is referenced in the Student Handbook.
* Compliance Monitoring and Reporting:	The policy is part of the Information Security Program and as such is audited annually by the Auditor of Public Accounts (APA). The ISO is responsible for promoting policy awareness and tracking compliance as part of the annual IT Security Awareness training.
RELATED INFORMATION:	
Policy Background:	
* Policy Category:	Information Technology
Category Cross Reference:	
Related Policies:	E.4.8. Monitoring of Employee Electronic Communications or Files
HISTORY:	
* Origination Date:	January 2005
* Approved by:	President Richard V. Hurley
* Approval Date:	January 1, 2005

* Effective Date:	January 1, 2005
* Review Process:	The effectiveness of this policy will be reviewed on an annual basis by the CIO or her/his designee.
* Next Scheduled Review:	July 1, 2014
Revision History:	7/1/2013 - added clarification to Purpose statement 1/31/2012 - revised to add test on review process and sanctions 6/18/2010 - updated to remove references to the Vice President for Strategy and Policy and add new language on file sharing 2/22/08 - updated to reflect change in responsible office for University-wide e-mail communications and change in language about changing passwords 4/16/07 - updated to reflect change in University-wide E-mail processes 8/21/06 - updated to reflect shift of responsibilities from Executive Vice President to Vice President for Strategy and Policy 1/10/05 - updated to reflect new policy formats, University name changes and other reference updates, and inclusion of user requirement for back-up of personal computers (originally in another University policy)

RFP ADDENDUM
February 24, 2014

ADDENDUM NO. 2 TO ALL OFFERORS:

Reference – Request for Proposals:	RFP #14-34
Commodity Code/to Furnish Goods or Service:	83845, 20854, 92014, 91829; POLICE CAD & RMS SYSTEMS SERVICES
Dated:	February 7, 2014
For Delivery to:	University of Mary Washington, Commonwealth of Virginia
Proposal Due Date:	**February 27, 2014; 3:00 PM**

This addendum consists of seven (7) pages.

ADDENDUM #2

I. Clarification to original RFP:

Below is a reference page for sellers to the Commonwealth of Virginia. There is an informational section listed which details reciprocity laws state-by-state.
http://www.eva.virginia.gov/pages/eva-i-sell-to-virginia.htm
A firm is not excluded from the RFP process even if the firm is not a VA certified small vendor, and does not intend to subcontract any of the work. If a vendor is not a certified Virginia Small Business it will not receive the 20 maximum points for small business certification or any fraction of the 20 points available or small business subcontracting if no data for subcontracting opportunities is submitted with the proposal. The proposal will still be evaluated against all of the remaining criteria outlined in the RFP.

II. Q & A from Offerors:

A. How many mobile units are you considering? Do you want Map and Routing on them?
The Police Department is considering three units; and this option (with or without Map and Routing) is pricing dependent (for a future contract term, based on budget).

B. Page 5: Item #4 - to what other specific agencies are you wanting to relay information to?
The RMS must be able to provide IBR reports to VSP and provide reporting information for the Clery Report (Campus Safety Report.

C. Page 5 Item B5 – what is the "Zone" system?
Zone is referring to areas in the UMWPD coverage area that are established as work areas to which officers could be assigned. When a call is entered, the officer for that area would be shown in the screen as the assigned office;, or if they are on a call, the next assigned officer

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

would be shown. It is understood by the UMWPD that GIS would have to be implemented for this option to work; however, if there is something that UMW needs in place before moving to GIS the vendor should provide information and pricing for it within the proposal.

D. Page 5 – Item #5, Are you looking for a PC based CAD and RMS system?
The Police Department requires a server/client based system and not an individual PC based system.

E. Page 6 Item #16 - in your $100,000:
   1. Does this also include the actual software and training for PROQA from Medical Priority? Most vendors can only offer an interface to their product, but you must license the software and get the training directly from Priority Dispatch.
   At this time we would not be Medical Priority dispatching; would like to add this in the future so our communication staff could be trained and give medical assistance to callers.

   2. Does it include the following for the AVL? The hardware, software, server & network routers, antennae, GPS receivers supported, wireless connection, etc.
   This is a section that would be completed in another phase; the funds are not currently available for the initial implementation.

F. Page 14 –Item 7.c – COOP Plan – what are you looking for in this? What other agencies are you looking to share data with?
The awarded contractor must have a plan in place for information surge and failure based on a large scale disaster/event. The firm should also have a business continuity plan that insures reliable response before, during, and after any large scale disaster. It should also include information regarding data recovery and back up.
UMW is not planning to share this data with any other agencies at present.

G. Is the University's current data scheme for the existing product for the UMWPD server-based?
Yes. The current system is server based and housed within the Police Dept; however, the new solution will need to be housed in the ITCC Data Center to centralize and protect it as we do all other systems.

H. Will the cost of any hardware come out of the budgeted $100k set aside for this project?
Yes. Whether the server is virtual or physical, we will need to supply new hardware from the project budget, based on the contractor's recommendations in conjunctions with University standards (per the RFP).

I. Is there Wi-Fi on campus?
Yes, but it is ubiquitous. Dorm wireless is provided by 3rd party and most of our green areas are not currently covered.

J. Can clarification be provided referencing the statement from the RFP regarding compliance with security policies; "If externally hosted, Contractor agrees to comply with all provisions of the then-current Commonwealth of Virginia Security Policy (SEC500-02) and Standards

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

(SEC501-01), published by the Virginia Information Technologies Agency (VITA). *Yes. UMW's network is in compliance with VITA's Security Policy. An offeror's solution must keep UMW in compliance with applicable VITA regulations and standards along with abiding by UMW policy and standards.*

K. RMS # 28 Does the College have a Live Scan machine to interface with? IF so what brand?
The University currently does not have Live Scan Equipment. It is interested in purchasing it at some point in the future.

L. RMS #31 Do you mean CAD system being proposed?
The RFP is for RMS and CAD. The University's Police Department must obtain as much information as possible from the current RMS (XRMS).

M. RMS# 32 what is the BossCars System?
The University uses this system for Parking Management. The initial installation does not need to integrate with BossCars. The University is interested in discovering if any CAD/RMS systems have integrated or can integrate with the BossCars system, possibly for future use. However, there is no intent to integrate with the BossCars system during this first phase.
http://www.bosssoftware.com/BOSSCARS

N. RMS# 525 What is Evidence on Q?
As mentioned during the pre-proposal conference, the University is using an RFP document that was originally developed for a county system with somewhat of a different scope. This item should be eliminated. The University does not have a current software program with evidence documentation and reporting capability. This RFP is to purchase such a system to include barcoding of evidence.

O. RMS#670 This is a requirement for pin mapping. An earlier question was answered that you do not use 911 type street addresses. Since pin mapping relies on valid street addresses, what is your expectation here?
During the pre-proposal conference, there was discussion regarding future use of GIS mapping. The University does not currently have 911 type street addresses and does anticipate having 911 street addresses in the near future. However, it is interested in some type of GIS mapping and does have some preliminary information that could be used in the future for this type of service. Please describe in the proposal what kind of capabilities are available in the offered system for GIS mapping.

P. RMS# 818 Prosecutor- This appears to be specifications for a court management system> Do you intend to strike this section?
The University does not currently have a prosecutor software package; however, if an offeror's solution contains a module that monitors cases that would go to the prosecutor, please include information and pricing within the response to the RFP. If priced as an "extra" option, it would likely not be part of the University's phase one implementation.

Q. RMS# 862- Again, This appears to be specifications for a court management system> Do you intend to strike this section?

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

See above.

R. CAD # 25-1177 Are you currently participating in the APCO/CSAA project and receiving alarms utilizing that method?
The University is a member of APCO but currently does not participate in any of the notification points.

S. CAD # 15-1140 You mention CAD MAP. Can you advise map creation platform and version?
There is limited UMW GIS data available for distribution. If offerors are capable of providing assistance with input of limited GIS/Google data that is presently available for upload, please provide this information in the RFP response. UMW does have facility points for GIS Data recorded.

T. CAD# 100-101- You answered earlier that you have no 911 capabilities. How do you want questions such as these answered?
As stated in the pre-proposal conference, please respond with a solution that is not associated with 911 capabilities.

U. CAD # 217- Do you currently have AVL capabilities?
No. Please provide information as to whether the solution being offered supports this feature as a potential future implementation for the University.

V. CAD # 261-262-476-1010 thru 1024. Do you currently do medical dispatch and use any of the referenced pre-arrival systems?
No. Please provide information as to whether the solution being offered supports this feature as part of the standard implementation or an add-on module for a future implementation.

W. CAD # 1185: Do you currently operate an EOC and do you use Web EOC?
The University does currently have its own EOC location, and is in the process of updating its EOC capabilities as well as relocating it to the new Information Technology Convergence Center (ITCC) project which will come online in June 2014. This is a potential alternative command center in a COOP situation. Although the University staff are trained in WEBEOC, by state statute an institution of higher education or state agency cannot declare an event; it must route through the local jurisdiction for support or enter requests through WEBEOC.

X. CAD # 1187: Is it your intent to run VCIC/NCIC inquiries directly from CAD?
Yes.

Y. The following CAD requirements appear to be duplicates. Can the University please provide additional details to differentiate them, or should these items be struck?
1. Row 86 appears to be a duplicate of row 84. *Yes, 86 is a duplicate.*
2. Row 879 appears to be a duplicate of row 867. *#879 is requesting the ability to create a report.*
3. Row 880 and 916 appear to be duplicates of row 868. *868 is the command list, 880 is the command report, 916 can be removed.*

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

4. Row 881 appears to be a duplicate of row 869. *No, 869 is the list and 881 is the report.*
5. Row 882 appears to be a duplicate of row 870. *No, 870 is the validation and 882 is the report.*
6. Row 904 appears to be a duplicate of row 877. *No, 904 is the listing and 881 is the report.*
7. Row 909 appears to be a duplicate of row 878. 909 is the listing and 878 is the report.
8. Row 929 appears to be a duplicate of row 888. *Yes, 929 can be removed.*
9. Row 931 appears to be a duplicate of row 886. *Yes, 931 can be removed.*
10. Row 932 appears to be a duplicate of row 887. *Yes, 932 can be removed.*

Z. The following CAD reporting requirements appear to actually be Tow functionality requirements. Can the University please confirm how these should be treated? (Row 860 – 866)
UMW performs a limited amount of towing; however, the University is desirous of a protocol to handle it more efficiently. Please indicate whether towing is a standard module of the CAD system, if not, please indicate and price a program that can integrate with CAD.

AA. Can the University please explain what Validation and Context is implied to mean for rows 870-875 of the CAD requirements?
This requirement is to ensure that rotation is followed by the protocol established.

BB. Row 1082 suggests that the system be capable of interfacing to APL systems. Due to the recent opinion of former Virginia State Attorney General Ken Cuccinelli that downloading information from Automated License Plate Readers is illegal; can the University please confirm that this is in fact a requirement or if this item should be struck?
This capability would not be part of the initial phase and may be considered for a future implementation.

CC. Row 1175 and 1176 appear to be requirements to interface to certain external systems, but do not list what those systems are. Can the University please confirm what those systems are, or if these requirements should be struck?
Please indicate other systems, if any, with which CAD/RMS may have integration capabilities. The CAD/RMS MUST integrate.

DD. The following Mobile requirement rows were blackened out. Can the University please advise if that was intentional or if a response is desired for these items (433, 447, 507)?
No response is required.

EE. Throughout this RFP, there were references made to interfacing to the Rappahannock Regional Jail. Can the University please confirm what system providers they use as well as what type of interface you would envision?
The Archonix system, as indicated in the pre-proposal conference, is currently being used by the University as part of a grant initiated by the RRJ. The University is desirous of a system that is able obtain and provide arrest information as necessary.

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

FF. Row 1017 (RMS) references an interface to the City of Fredericksburg Court Records. Can the University please confirm what system providers they use, and define what type of interface it is that you would envision?
This requirement is not needed in the initial implementation; however, the University is desirous of potentially supporting the interfacing with a court system for a future implementation.

GG. There are multiple Mobile references to "automated field reports", does this just refer to mobile field reporting?
Yes.

HH. Mobile – Problem Oriented Policing – ability to create community policing record. Does this refer to something other than a CAD or incident report?
No, it refers to CAD/incident reports.

II. Mobile – Report Validation/Submission- is this a requirement to do NIBRS submission to the VSP from a mobile unit instead of the central RMS system?
The intent of this requirement specification is to have the ability to validate/submit reports from a vehicle to the UMW system and that the UMW system would be able to report NIBRS submission to VSP from UMW's central RMS system.

JJ. RMS – 172 –Does RMS perform a matching function using a rules based process defined by the agency? Could you please provide some clarification on what exactly is being asked?
This requirement specification is regarding the ability to create different rules for searching in the master name list. Please detail other search types outside of the standard search protocol.

KK. RMS 654- What is meant by Generic Permits?
Can the offeror's proposed system create and track different styles of permits; including but not limited to Bike registration, student property forms, parking permits, etc.?

LL. ANi/ALI data is listed as a requirement, but indications seem to exist that the University is not on a standard 911 ANI/ALI feed. Is the telephone system providing standard compliant ANI/ALI data or is it proprietary format?
This is correct. The University does not currently have ANI/ALI feed capability.

MM. CAD 479 – Ability to meet FERPA and HIPPA requirements for data security where appropriate. Could you provide more specifics as to what requirements you expect CAD to provide related to the call data?
The University requires that all protected information (highly sensitive data) is secured at all times per:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168

END OF ADDENDUM #2

Melva Kishpaugh, VCO
Asst. Director, Procurement Services
Phone: 540/654-1084

*Acknowledged receipt of RFP 14-34 Addendum #1 (and all addenda) should be acknowledged and included in the RFP submittal package:

_____ _____
SIGNATURE DATE

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu/purchasing
Tel: 540/654-1127
Fax: 540/654-1168