JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU5758**

This contract entered into this 2nd day of April 2020, by Assura, Inc., hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

WITNESSETH that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From April 2, 2020 through April 1, 2021 with four (4) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposal FDC-1057 dated September 19, 2019:
  (a) The Statement of Needs,
  (b) The General Terms and Conditions,
  (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
  (d) Addendum One, dated October 9, 2019.

(3) The Contractor's Proposal dated October 24, 2019 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
  (a) Negotiations Summary, dated February 14, 2020.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By: _____ (Signature)	By: _____ (Signature)
Karen L. Cole (Printed Name)	Doug Chester (Printed Name)
Title: CEO	Title: Buyer Senior

Rev. 10/14/09

RFP # FDC-1057
Information Technology Security Auditing Services
Negotiation Summary for Assura, Inc.
February 14, 2020

1. The pricing schedule is as follows:

Labor Category	Off-site Rate	On-site Rate
Principal Threat Intelligence Consultant	$237.63	$256.50
Senior Threat Intelligence Consultant	$203.91	$223.25
Quality Assurance Consultant	$179.42	$195.70
Security Tester I	$81.57	$97.85
Security Tester II	$114.17	$131.10
Security Tester III	$130.49	$147.25
Security Tester IV	$146.81	$163.40
Security Tester V	$163.12	$179.55
Security Auditor I	$81.57	$97.85
Security Auditor II	$97.89	$97.89
Security Auditor III	$114.17	$131.10
Security Auditor IV	$130.49	$147.25
Security Auditor V	$146.81	$163.40
Security Engineer I	$122.35	$138.70
Security Engineer II	$146.81	$163.40
Security Engineer III	$179.42	$195.70
Project Manager I	$81.57	$97.85
Project Manager II	$97.89	$97.89
Project Manager III	$114.17	$131.10

   All rates in the pricing schedule are inclusive of travel.

2. The University may also request that these services be provided as a fixed-fee project, as would be mutually agreed to prior to services being rendered, with deliverables billed upon completion of milestones

3. Contractor has disclosed all potential fees. Additional charges will not be accepted.

4. The University may also request that these services be provided as a monthly subscription service, as would be mutually agreed to prior to services being rendered, with deliverables determined by monthly service requirements.

REDACTED

Information Technology
Security Auditing Services
RFP# FDC-1057

Prepared for

JAMES MADISON
UNIVERSITY

Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Bldg.
First Floor, Suite 1023
Harrisonburg, VA 22807

Prepared by

ASSURA
Assura, Inc. • 7814 Carousel Lane • Suite 202 • Richmond, Virginia 23294
(866) 672-8714 • **www.assurainc.com**

Please note that per § 2.2-3700 et. seq of the Code of Virginia, all information underlined in this Statement of Work are trade secrets as defined under the Uniform Trade Secrets Acts and are proprietary and confidential to Assura.

REDACTED

Information Technology Security Auditing Services

RFP# FDC-1057

Prepared for

JAMES MADISON UNIVERSITY

Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Bldg.
First Floor, Suite 1023
Harrisonburg, VA 22807

Prepared by

ASSURA

Assura, Inc. • 7814 Carousel Lane • Suite 202 • Richmond, Virginia 23294
(866) 672-8714 • **www.assurainc.com**

ASSURA INC

October 24, 2019

Mr. Doug Chester, Buyer Senior
Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

RE: Request for Proposal # FDC-1057 Information Technology (IT) Security Auditing Services

Dear Mr. Chester:

It is our pleasure to submit our response to RFP # FDC-1057 Information Technology (IT) Security Auditing Services. We appreciate the opportunity to potentially expand our work with James Madison University (JMU) and other Virginia Association of State and College University Purchasing Professionals (VASCUPP) organizations to assist in their continued efforts in identifying and remediating security vulnerabilities. As evidenced by JMU's description of services performed by the Audit Management Service Department as well as the issuance of this RFP; the organization understands the critical need to maintain reasonable assurances to management and key stakeholders that prudent measures are consistently taken to identify and mitigate security risk to systems and data utilized.

Our proposal will demonstrate our significant experience in the industry and the talents we can bring to JMU and other VASCUPP organizations if awarded this contact. We thank you in advance for JMU's time and consideration of our proposal.

If you have any questions or if I may be of assistance, please do not hesitate to contact me at (804) 767-4521 or karen.cole@assurainc.com

Sincerely,

Karen L. Cole
CEO

7814 Carousel Lane, Suite 202
Richmond, VA 23294
Telephone: 804-672-8714
Toll Free: 855-9NOHACK

Table of Contents

1. RFP Acknowledgements

REQUEST FOR PROPOSAL

RFP# FDC-1057

Issue Date: **September 19, 2019**

Title: **Information Technology (IT) Security Auditing Services**

Issuing Agency: **Commonwealth of Virginia**
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on October 17, 2019 for Furnishing The Services Described Herein.

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.

In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

7814 Carousel Lane

Suite 202

Richmond, VA 23294

By: _____ *(Signature in Ink)*

Name: Karen L. Cole *(Please Print)*

Date: October 24, 2019

Title: Chief Executive Officer

Web Address: www.assurainc.com

Phone: 804-767-4521

Email: Karen.cole@assurainc.com

Fax #: 804-672-6442

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 KLC #2 ____ #3 ____ #4 ____ #5 ____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
☑ YES; NO; *IF YES* ⇒⇒ ☑ SMALL; ☑ WOMAN; MINORITY ***IF MINORITY:*** AA; HA; AsA; NW; ☑ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

2. Mapping of RFP Requirements

Section	Section Title	RFP Section V Mapping and Description	Proposal Page Number
1	RFP Acknowledgements	• Maps to V.B.1 • RFP Cover Sheet and All Addenda Acknowledgements	1
3	Goods and Services Plan and Methodology	• Maps to V.B.2 • Response to Statement of Needs	3
4	Firm Overview and Qualifications	• Maps to V.B.3 • Response to Expertise, Qualifications, and Experience of Firm • Resumes of Key Personnel	26
5	Offeror Data Sheet	• Maps to V.B.4 • Attachment A from RFP	29
6	Small Business Subcontracting Plan	• Maps to V.B.5 • Assura SWaM Certification	30
7	VASCUPP Sales	• Maps to V.B.6	32
8	Proposed Cost	• Maps to V.B.7 • Pricing Schedule	33
9	Additional Information	• Maps to V.A.3.C • Additional Material	34

3. Goods and Services Plan and Methodology

James Madison University (JMU) continues to set the standard of excellence in higher education as evidenced by being rated the 2019 #1 most innovative university in the South by U.S. News and World Report. In addition, JMU has been long recognized as developing one of the original seven National INFOSEC Education and Training Program centers in the United States. These centers were designated by the National Security Agency and the Department of Homeland Security for universities that demonstrate academic excellence in information assurance education. It is a significant accomplishment to be recognized by the United States government as furthering the profession of information security for the next generation.

It is this forward thinking that has also resulted in JMU being the driving force behind developing statewide contract vehicles that ease the pain of obtaining cyber security services for members of the Virginia Association of State College and University Purchasing Professionals (VASCUPP) as well as other government and quasi-government entities. These efforts demonstrate that JMU is committed to ensuring that not only are their students, staff, sensitive data, and critical systems are protected from cyber security threats and vulnerabilities; but their colleagues in other Virginia organizations as well.

Assura is pleased to provide this response to RFP# FDC-1057 Information Technology (IT) Security Auditing Services that demonstrates our unparalleled knowledge to deliver security assessment and testing services as well as our superior work quality, outstanding results, and reasonably priced options to meet all of JMU and VASCUPP's security audit needs.

Statement of Needs

Assura stands at the ready to provide experienced and certified individuals to meet the needs of JMU and VASCUPP members. Since the beginning of the firm in 2007, Assura has been providing security assessment and testing services for Virginia government and institutions of higher education. Assura only utilizes personnel on engagements that have an applicable certification to the work performed. This includes, at a minimum, the following certifications:

- CISSP – Certified Information Systems Security Professional from ISACA
- CISM – Certified Information Security Manager from ISACA
- CISA – Certified Information Systems Auditor from ISACA
- CEH – Certified Ethical Hacker from EC-Council
- CRISC – Certified in Risk and Information Systems Control
- Security+ - Security Certification from CompTIA

In addition to performing successful security assessments and training projects, Assura also performs information security auditing services. As such, Assura is pleased to have its own Red Book compliant auditing program. This demonstrates that Assura embraces the core tenants of audit and can easily ensure that our services augment any audit initiative.

It is Assura's commitment to controls excellence that is carried throughout all of our services. As such, Assura is the only firm to have AuditArmor™ & Audit Defense™ guarantees.

> **AuditArmor™** is a 100% guarantee that our work is always compliant with the identified standards and regulations and will stand up to the scrutiny of audit. If our work is deemed noncompliant for any reason, then we will fix it for free. *In the almost 13 years Assura has been in business, we have never had to fix our work!*
>
> **Audit Defense™** promises that we will work with auditors and regulators to defend our work and prevent unnecessary findings – free of charge for services that we have provided. The least risky part of security services should be selecting the provider.

The remainder of this section details how Assura's services address the needs of JMU and VASCUPP members.

C.1.a: External Vulnerability Assessment

Assura's Managed Vulnerability Scanning and Management service utilizes tools such as Tenable Nessus, Veracode Dynamic Scan, and ServerScan for scanning by a PCI Approved Scanning Vendor (ASV). The scope of our scans includes:

- Device and application discovery;
- Vulnerability identification and scoring; and
- Compliance assessment and scoring.

Our vulnerability assessments not only uncover security flaws from outdated software, they uncover insecure hardware and software configurations such as variances from Center for Internet Security Benchmark controls, and application level flaws such as injection, cross-site scripting, and request forgery vulnerabilities. We can also integrate static code analysis tools to identify and manage vulnerabilities in custom applications and third-party libraries such that it integrates seamlessly with each client's system development life cycle, change control, and release management practices.

CIS® Center for Internet Security®

Each vulnerability is then scored using the Common Vulnerabilities Scoring System (CVSS) or the Common Weaknesses Scoring System (CWSS).

Once a vulnerability is identified and scored, we work with the client's security and IT operations to confirm the vulnerabilities and assist them with expert guidance for remediation on a prioritized basis. We also have the means of configuring our system to automatically alert IT operations of a critical vulnerability through their service management platform.

Vulnerabilities are then mapped to the client's asset inventory with critical assets scheduled for remediation of high impact vulnerabilities first.

At the client's option, we can report on the status of vulnerability remediation and newly identified vulnerabilities at a tempo that's right sized for the organization.

Deliverables

- Continuous vulnerability identification and monitoring.
- Prioritized, automated testing and deployment of security patches.
- Assistance with remediation of vulnerabilities that cannot be corrected with a security patch.
- Vulnerability severity distribution.
- Vulnerability remediation status.

Reports (monthly or more frequently) on configuration compliance for PCI DSS, HIPAA, and others.

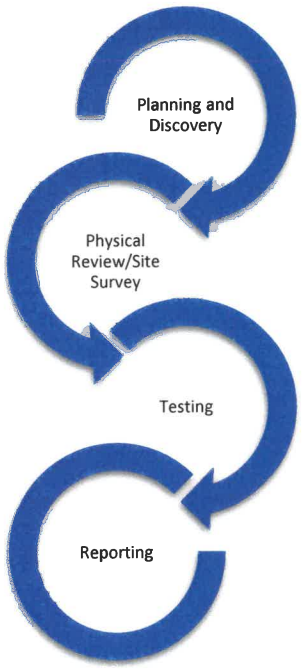
C.1.b: Wireless Network Assessment

Our wireless penetration testing methodology is broken down into four phases, as described below.

Planning & Discovery

Before beginning testing, we conduct a brief meeting with the client to review and acknowledge the penetration testing rules of engagement, confirm project scope and testing timeline, identify specific testing objectives, document any testing limitations or restrictions, and answer any questions related to the project.

Assura begins each assessment by performing a walkthrough of all in-scope facilities in order to enumerate advertised and hidden wireless networks and the physical location of access points. At the conclusion of this phase Assura generates a wireless network inventory that lists the wireless network name, encryption, and associated access point MAC address. Assura then confirms all in-scope wireless networks with the client's team, including MAC addresses and SSIDs. This assists in confirming the presence or absence of rogue access points.



Physical Review/Site Survey

Assura uses the inventory generated during the Planning & Discovery phase to locate and inspect access points that may be in publicly accessible locations. If found, Assura inspects the access point for open console or ethernet ports and validates if they provide access to sensitive networks or to the management console of the access point. Using several high-gain antennas, our testers walk the perimeter of the network and track the various wireless signals throughout the organization. Additionally, the tester will walk outside of the facility and continue to collect signals. This allows the tester to correlate whether a particular access point is within the client's network, or a nearby network. The tester will then determine whether the wireless signal is significantly leaking outside of sensitive areas that could allow an attacker to target the wireless network from nearby locations. In addition to taking an inventory of available SSIDs and measuring signal strength, the tester will also be searching for rogue access points within the building.

Testing

For any networks that use WEP, WPA, WPA2-PSK, or WPA3-PSK encryption, Assura passively monitors wireless traffic and captures authentication information. Assura uses captured authentication traffic to attempt an offline brute force attack to determine if the passphrase is sufficiently strong. For any networks that use a weak passphrase or don't use encryption Assura associates with the wireless network and perform the following tasks:

- Collect basic network information including internal network range, DHCP / DNS configurations, external IP address, and filtering on network traffic (e.g. URL filtering, malware filtering, port blocking).
- Determine other network ranges that may be accessible from the attached network.
- Determine if client isolation is enabled on the network.
- Determine if broadcast filtering is enabled on the network.
- Check if network infrastructure management services are accessible from the network such as access point management interfaces or router SSH/telnet ports.
- Determine if corporate assets are accessible from the network by monitoring traffic.
- Determine if unencrypted traffic discloses sensitive information (e.g. SNMP strings, usernames, passwords).

Optionally, Assura can perform active testing including:

- Targeting WPA2-Enterprise protected networks using an "Evil Twin" attack. This testing is used to validate if endpoints are properly configured to validate the access point their associating with. If vulnerable this will result in gaining access to authentication information for endpoints or users.
- Use social engineering techniques to advertise similarly named wireless networks with crafted captive portal pages designed to capture username and passwords from employees.
- Vulnerability scans performed against any associated networks. This identifies systems that could potentially be attacked and used to gain further access into the environment.
- LLMNR/NBT-NS poisoning attacks on any associated network to potentially gain authentication information of other systems on the network.

<u>Reporting</u>

The wireless testing report provides:

- An overview of the scope of the testing
- Testing methodology
- Signal heat maps of client SSIDs that identify areas of signal or SSID leakage
- Inventory of discovered access points and SSIDs and protective mechanisms
- Findings and recommendations to correct identified vulnerabilities

Assura also provides an executive-level out-brief as part of its reporting.

C.1.c: Firewall and Router Security Assessment

Assura's firewall and router configuration security assessments have been conducted for clients such as Sheltering Arms and the Virginia Retirement System. Our assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices or devices where end-of-life is imminent;
- Ports, protocols, and services permitted by policy to be routed through the firewall or router;
- Access control list alignment with policies to ensure that data flows are enforced per approved configurations;
- Vulnerable configurations, software, and firmware;
- Configuration security of the device itself in accordance with Center for Internet Security benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs);
- Use of a dedicated management Virtual Local Area Network (VLAN) to isolate access to management functions;
- Credentials and keys such as passwords, multifactor authentication, SSH keys, and Simple Network Management Protocol (SNMP) strings are provisioned, implemented, and managed in accordance with best practices;
- OS/firmware patch level to identify any open security or functionality issues;
- AAA (centralized authentication, authorization, and audit) on all devices;
- Other configuration-related items (e.g., URL filtering, content inspection, and Intrusion Prevention System configuration) for Unified Threat Management devices; and
- Other items.

Assura's methodology for firewall and router security assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as device security policies; configuration standards; approved ports, protocols, and services; and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with network administrators, and through the use of automated tools such as Nessus and CIS-CAT to identify variances from industry best practices as well as other weak configuration or vulnerabilities. We then provide a score of each device's security so that the client has concrete metrics to show compliance with industry practices.

Reporting

The firewall and router security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed devices, including name, make, model, serial number, operating system version, and primary IP address
- Testing methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

Assura also provides an executive-level out-brief as part of its reporting.

C.1.d: Server Configuration Assessment

Assura's server configuration assessments are similar to its firewall and router configuration security assessments. We have conducted this type of assessment for clients such as the REDACTED. Our assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices or devices where end-of-life is imminent;
- If the server is a hypervisor host, support by the hypervisor OEM, including end-of-life versions or versions where end-of-life is imminent;
- If the server is in a cloud Infrastructure-as-a-Service (IaaS) provider, security best practices for the cloud tenant such as encrypted volumes, Identity and Access Management keys and roles, and use of security services provided by the IaaS provider (e.g., Amazon Guard Duty and Security Hub);
- Approved software and functions for the server;
- Ports, protocols, and services permitted by policy to be processed by the server;
- Access control list alignment with policies to ensure that data flows are enforced per approved configurations;
- Configuration security of the server and services (e.g., IIS, Apache, SQL, Oracle, etc.) in accordance with Center for Internet Security benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs);
- Use of malware defense, Host-based Intrusion Detection/Prevention, firewall, and Endpoint Detection and Response (EDR);
- Use of a dedicated management Virtual Local Area Network (VLAN) to isolate access to management functions such as IPMI ports;
- Credentials and keys such as passwords, multifactor authentication, SSH keys are provisioned, implemented, and managed in accordance with best practices;
- OS/firmware patch level to identify any open security or functionality issues; and
- Other items.

Assura's methodology for server configuration assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as device security policies; configuration standards; approved server roles; approved ports, protocols, and services; and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with system administrators, and through the use of automated tools such as Nessus and CIS-CAT to identify variances from industry best practices as well as other weak configuration or vulnerabilities. We

then provide a score of each device's security so that the client has concrete metrics to show compliance with industry practices.

Reporting

The server security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed devices, including name, make, model, serial number, operating system version, and primary IP address
- Testing methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

Assura also provides an executive-level out-brief as part of its reporting.

C.1.e: Database Architecture Security Assessment

Assura conducts database architecture security assessments review the way that databases are constructed, data is protected, database segmentation, data is accessed, and how databases are monitored. We conduct assessments of databases built on Oracle, Microsoft SQL Server, MySQL, PostgreSQL, NoSQL, MongoDB, MariaDB, and others. We can do assessments of traditional DBMS installations or on fully managed services such as Amazon Relational Database Service (RDS) or Microsoft Azure Databases. We do assessments for databases, data warehouses, and data lakes as well as security of BLOB storage such as in Amazon Simple Storage Service (S3) buckets.

Our assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life software or software where end-of-life is imminent;
- Database roles and account permissions;
- Data segmentation (logical and physical) based on regulatory and policy requirements;
- Availability including backup and replication;
- Data protection such as hashing, encryption, masking, and tokenization;
- Use of production data in non-production environments;
- Auditing and logging;
- Configuration compliance with best practices such as CIS Benchmarks;
- Monitoring for data-layer attacks, exfiltration, and misuse of data; and
- Other items.

We use tools such as Nessus, the Oracle Database Security Assessment Tool (DBSAT), and the SQL Vulnerability assessment capabilities built into SQL Server Management Studio for SQL Server 2012 and later.

Assura's methodology for database architecture security assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as data security policies; business impact analysis; data classifications; configuration standards; and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with database administrators, and through the use of automated tools.

Reporting

The server security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed databases
- Assessment methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

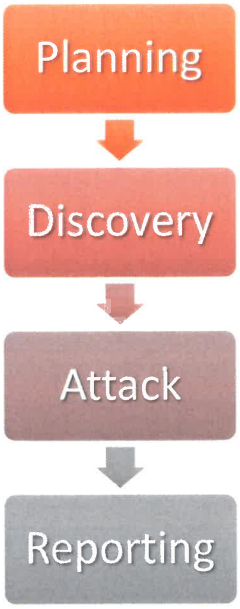
Assura also provides an executive-level out-brief as part of its reporting.

C.1.f: Network Scanning Process Assessment

Assura uses a proven four-phase process to conduct network scanning.

Planning

The Planning phase is where Assura obtains targeting information from the client. This includes IP addresses of specific devices and/or network/subnetwork addresses. We also request that the client provides us with a list of devices and/or subnets/VLANs known to be sensitive to scanning so that they can be excluded from scanning or scanned separately with the production support staff for those devices on standby in case an issue arises.



Scanning

In the Scanning phase, Assura configures the scanning software tools with the targets and ensures that only non-destructive scanning is performed. The scanners will then identify known vulnerabilities using signature patterns. The purpose of these scans is to identify unnecessary services, unusual use, vulnerable software, and active vulnerabilities. Assura will not attempt to exploit any of the vulnerabilities identified in this activity.

Analysis

The Analysis phase is where Assura uses its expertise to identify critical vulnerabilities that need to be reported immediately; identify potential false positives[1]; and identify patterns and trends that need to be highlighted in the Reporting phase. The team will also map identified services to server functions in order to properly identify which running services are superfluous, increase the attack surface of the device, and/or pose a high risk.

Reporting

The Reporting phase consists of developing and delivering two reports:

1. An Executive Report that provides a management-level overview of the results of the assessment including key findings such as critical vulnerabilities and trends, and recommendations for remediation. Recommendations may include software updates, configuration changes, process changes, additional training for IT personnel or a combination of those.
2. A Detailed Assessment Report that provides in depth information about each vulnerability along with a Common Vulnerability Scoring System (CVSS) base score. Assura uses CVSS scores because they provide an easy-to-understand metric that represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments and expresses the potential impacts to

[1] While every attempt will be made to identify and discard "false positive" results through post-test review of the data, additional "false positives" may be revealed as the client and Assura conduct further analysis to address identified weaknesses.

confidentiality, integrity, and availability of data. If warranted, Assura may also calculate the temporal and environmental scores in order to better communicate the magnitude of risk in the context of the client's IT environment and threat landscape. The report also provides detailed information about how to remediate each vulnerability.

Clients such as Commonwealth Public Broadcasting Corp (Virginia's Home for Public Media – formerly Community Idea Stations), University of Mary Washington, and many others have all benefitted from Assura's proven approach.

C.1.g: Web Application Security Assessment

Assura's approach to external web application penetration testing utilizes a combination of automated (for applications where automated testing is safe) and manual testing techniques.

For those applications where it is safe to utilize tools, Assura uses a combination of open source and commercial tools. Examples of the tools we use are Burp Suite, SQL Map, Dirbuster, Nikto, and Veracode Dynamic Scan. We use each tool to identify flaws that can be exploited such as privilege escalation, non-sanitized inputs, etc. that could lead to compromise of data and information resources.

Although tools reveal some potential avenues of attack, there is nothing like hands-on attempts to find and exploit flaws. With these methods, Assura can find instances where clear text passwords are being stored by the system, privilege escalation, data leakage, and weaknesses that allow target systems to be used to attack other organizations. Assura's expert testers know how to identify and exploit even the most subtle application flaws.

Assura conducts web application security assessments for clients such as University of Mary Washington, West Creek Financial, the County of York, Virginia and others. We do application-focused anonymous tests as well as authenticated tests to identify exploitable vulnerabilities that can lead to privilege escalation, compromise of data segmentation, and data exfiltration. We also do full stack assessments to identify weaknesses at all levels of an application. Our assessments analyze and evaluate the following security-related components:

- Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks;
- CWE/SANS Top 25 Most Dangerous Software Errors;
- Payment Card Industry Data Security Standard (PCI DSS) Requirement 6;
- Server-side Request Forgeries;
- Information disclosures; and
- Many others.

Assura's methodology for web application security assessment consists of four phases, as described below:

<u>Planning</u>

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE act as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized);
- Prerequisites (e.g., systems operating normally);

- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact;
- Test parameters (e.g., authorized test activities);
- IP address(es) where testing originates;
- List of applications to be tested (by URL);
- Handling of sensitive information to prevent unauthorized disclosure;
- Destruction of sensitive information that comes into the possession of the test team;
- Methods and timing for reporting sensitive information;
- Process for halting operations;
- A de-confliction process; and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window.

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities using automated tools such as Burp Suite and Veracode Dynamic Scan.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to identify application weaknesses and test whether the application addresses common vulnerabilities such as the OWASP Top 10 and CWE/Sans Top 25.

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

During the attack stage, the client's attack sensing and warning capability may also be challenged.

Reporting

The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of: EXPOSURE, CONCERN, or INFORMATIONAL along with a CVSS score.

For each identified weakness Assura will, recommend detailed remediation steps. This could include application of security patches, changing a system setting (or set of settings), implementing/modifying a compensating control or modifying application code (right down to the function call).

Each report includes the following:

- Executive Summary written to be understandable by non-technical personnel;
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test;
- Detailed description of each vulnerability; and
- Evidence of system access with screen shots of compromise redacted of sensitive information.

Assura will conduct up to one retest of any weaknesses identified as and exposure or concern within 90 days of delivery of the final report.

C.1.h: Active Directory Security Assessment

Active Directory Security Assessments attempt to identify weaknesses that can lead to account and system compromise. Assura has conducted this type of assessment for clients such as VCU Health. We use tools such as SMBMap, crackmapexec, responder, PowerView, and mimikatz. Our assessments analyze and evaluate the following security-related components:

- Active Directory metadata dump;
- Weak credentials;
- Weak permissions;
- Insecure server configurations; and
- Many others.

Assura's methodology for Active Directory security assessment consists of four phases, as described below:

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE act as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized);
- Prerequisites (e.g., systems operating normally);
- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact;
- Test parameters (e.g., authorized test activities);
- IP address(es) where testing originates;
- List of applications to be tested (by URL);
- Handling of sensitive information to prevent unauthorized disclosure;
- Destruction of sensitive information that comes into the possession of the test team;
- Methods and timing for reporting sensitive information;
- Process for halting operations;
- A de-confliction process; and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window.

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities using automated tools such as SMBMap and PowerView.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to identify weaknesses that permit account compromise, access to unauthorized information, injection of code, and other weaknesses.

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

During the attack stage, the client's attack sensing and warning capability may also be challenged.

Reporting

The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of: **EXPOSURE**, **CONCERN**, or **INFORMATIONAL** along with a CVSS score.

For each identified weakness Assura will, recommend detailed remediation steps.

Each report includes the following:

- Executive Summary written to be understandable by non-technical personnel;
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test;
- Detailed description of each vulnerability;
- Detailed timeline of the test identifying each test step; and
- Evidence of system access with screen shots of compromise redacted of sensitive information.

Assura will conduct up to one retest of any weaknesses identified as and exposure or concern within 90 days of delivery of the final report.

C.1.i: Penetration Testing

Whether internal or external; white, grey box, or black box; no matter the target type (application, network, hardware, software); and no matter if the test strictly focuses on technical testing or includes social engineering, Assura uses a penetration testing methodology to address those needs. We do penetration testing for clients such as County of York Virginia, Apex Systems, University of Mary Washington, Virginia Department of Emergency Management, and others.

Approach and Methodology

Assura's approach and methodology is based on a combination of National Institute of Standards and Technology (NIST) Special Publication 800-115 and The Open Source Security Testing Methodology Manual (OSSTMM). As such, our certified professional staff utilizes a four-stage penetration testing methodology as represented in Figure 4.

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE act as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized);
- Prerequisites (e.g., systems operating normally);
- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact;
- Test parameters (e.g., authorized test activities);
- IP address(es) where testing originates;
- List of user populations, facilities and/or IT applications to be tested;
- Handling of sensitive information to prevent unauthorized disclosure such as:
    - Utilizing whole disk encryption on all laptops that store sensitive information;
    - Sensitive information is placed on removable media is stored on FIPS 140-2 validated encrypted media;
    - Electronic Mail messages that contain sensitive information are encrypted using OME;
    - Large files are transmitted using either Secure File Transfer Protocol (SFTP) or via Citrix ShareFile;
- Destruction of sensitive information that comes into the possession of the test team;
- Methods and timing for reporting sensitive information;

- Process for halting operations;
- A de-confliction process; and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window.

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities using automated tools and/or Open Source Intelligence (OSINT) about the organization and its personnel. Some of the means we use in the discovery stage include but are not limited to:

- Google Hacking – Utilizing Google and other search engines to identify potentially useful information that could provide the team with a means of discovering information that could be used to disclose sensitive information such as passwords or information that could be used as information to perform password reset. This could allow the team to change user credentials and gain access into a system.
- Social Media Exploration – This discovery technique could permit the team to find further information that could lead to a successful compromise of a system. It could also be used to find information that could then be used as enticement for a user to disclose otherwise privileged information.
- Discovery of Web Sites and Internet Connectivity – This phase of discovery will utilize a number of tools such as Veracode Discovery to search DNS records, known IP address space and search engines in an attempt to identify web sites and internet connectivity points.
- Port scanning, fingerprinting, and vulnerability identification. The team will use automated tools such as Nessus Vulnerability Scanner, Nmap, and OpenVAS to conduct this reconnaissance.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to:

1. Elevate privileges on target systems in order to gain high level access (e.g., administrative) to system functions;
2. Use access to systems where the team has gained entry to attack other systems through transitive trust; and
3. Use the information obtained through items 1 and 2 to identify the information that can be compromised from the standpoints of confidentiality, integrity and/or availability.

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

During the attack stage, the client's attack sensing and warning capability will be challenged. Whether the Assura team's exploits are discovered and potentially acted upon will be an excellent test of that capability.

Reporting

The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of: **EXPOSURE**, **CONCERN**, or **INFORMATIONAL** along with a CVSS score.

For each identified weakness Assura will, recommend detailed remediation steps. This could include application of security patches, changing a system setting (or set of settings), implementing/modifying a compensating control.

Each report includes the following:

- Executive Summary written to be understandable by non-technical personnel;
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test;
- Detailed description of each vulnerability; and
- Evidence of system access with screen shots of compromise redacted of sensitive information.

Assura will conduct up to one retest of any weaknesses identified as and exposure or concern within 90 days of delivery of the final report.

C.1.j: Telecommunications

Telecommunications penetration testing such as identifying exploitable weaknesses in Voice Over IP (VoIP) implementations helps to identify areas where communication confidentiality can be compromised as well as leaving an organization open to call tracking, call data manipulation, toll fraud and other scams. Assura's telecommunications assessments are similar to traditional penetration tests where the VoIP infrastructure is attacked. We use tools such as Nmap, Metasploit, rtpbreak, siparmyknife, and others. Our telecommunications assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices, software, and firmware or devices, software, and firmware where end-of-life is imminent;
- Unpatched vulnerabilities in VoIP infrastructure equipment;
- Uncredentialed access to Session Initiation Protocol (SIP) proxies;
- Weak credentials to SIP proxies;
- Use of unencrypted communications with SIP proxies;
- Vulnerability to man-in-the-middle attacks to decode G.711 traffic and eavesdrop on communications;
- RTP injection;
- Voicemail attacks
- Adequate network segmentation;
- Quality of Service (QoS); and
- Others.

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE act as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized);
- Prerequisites (e.g., systems operating normally);
- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact;
- Test parameters (e.g., authorized test activities);
- IP address(es) where testing originates;
- List of applications to be tested (by URL);
- Handling of sensitive information to prevent unauthorized disclosure;
- Destruction of sensitive information that comes into the possession of the test team;
- Methods and timing for reporting sensitive information;
- Process for halting operations;
- A de-confliction process; and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window.

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities using automated tools such as Nmap and Metasploit's SIP enumerator.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to identify weaknesses that permit account compromise, access to unauthorized information, injection of code, and other weaknesses.

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

During the attack stage, the client's attack sensing and warning capability may also be challenged.

Reporting

The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of: **EXPOSURE**, **CONCERN**, or **INFORMATIONAL** along with a CVSS score.

For each identified weakness Assura will, recommend detailed remediation steps.

Each report includes the following:

- Executive Summary written to be understandable by non-technical personnel;
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test;
- Detailed description of each vulnerability;
- Detailed timeline of the test identifying each test step; and
- Evidence of system access with screen shots of compromise redacted of sensitive information.

Assura will conduct up to one retest of any weaknesses identified as and exposure or concern within 90 days of delivery of the final report.

4. Firm Overview and Qualifications

Assura was created as a Virginia corporation in 2007 with the mission of securing the future one client at a time and the vision of democratizing cyber security. At Assura, we believe that security of data and systems is a right and not a privilege. It is this belief that has allowed the firm to continue to grow and prosper over our 12 years in business.

We believe that state-of-the-art cyber security solutions should be available for institutions of higher education and government organizations regardless of limited budgets. As JMU and other VASCUPP organizations are preparing America's youth for the future, Assura supports their mission by ensuring that their future is protected from malicious threat actors and data breaches with cost-friendly solutions.

At Assura, our mission is to democratize cybersecurity because everyone deserves to have their data and systems protected.

To this end, we focus on providing services and tools to meet the most complex cyber security needs at the right price.

In September 2019, Assura performed a service satisfaction survey for our current clients and the feedback was outstanding. Our results show:

- **91%** of current clients rate Assura service 4+ out of 5 in overall satisfaction.
- **73%** of our clients rated their spend with Assura as "5 – Best Dollar for Dollar I've Spent" or "4 – My Dollar Went Further Than I Thought."
- **64%** of respondents said that Assura's services went "Outstanding - Above and Beyond What We Needed" or "Exceeds Expectations - More Than We Needed"
- **90%** of respondents indicated that Assura is extremely responsive to their requests and needs.

Since our first day in business, Assura only utilizes personnel with industry certifications in their cyber security service area.

Socio-Economic Overview

Assura is a Richmond, Virginia based small-woman-owned cyber security advisory and managed services firm. Our company is proud to be a certified as a:

- Small Woman and Minority Owned (SWaM) certified Small, Woman-Owned business by the Virginia Department of Minority Business Enterprises (Certification # 661749);
- Women's Business Enterprise (WBE) by the prestigious Women's Business Enterprise National Council (WBENC) (Certification # 2005124455); and an

- Economically Disadvantaged Woman Owned Small Business (EDWOSB) by the U.S. Small Business Administration.

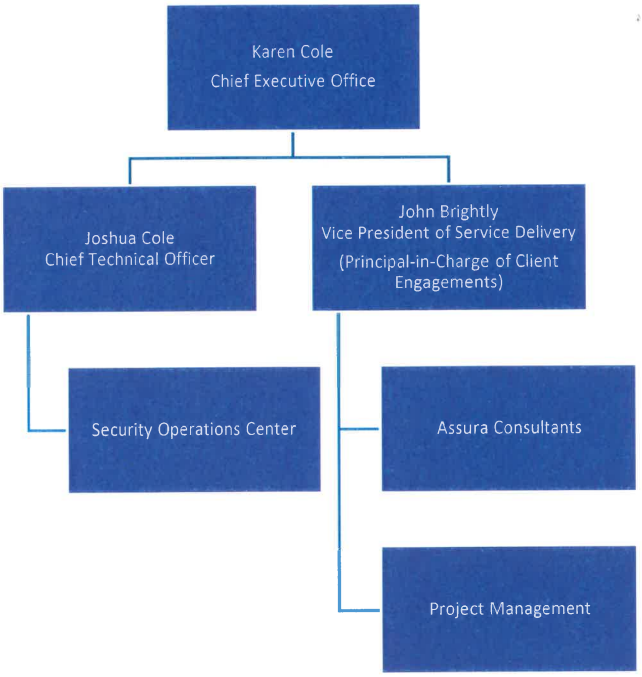
Assura has been identified as being in the top 1% of women-owned firms in the United States by the U.S. Women's Chamber of Commerce. This metric was derived from evaluation of business assets, management structure, and controls that ensure the organization is well-managed

Assura is pleased to have been awarded the JMU contract for cyber security consulting services in 2018. Over the past 12 months, various universities and government organizations have already taken advantage of the easy-to-use contract when they have needed general cyber security planning. It is our sincere hope that JMU will allow us to provide even more cyber security services throughout the Commonwealth of Virginia and beyond with the award of this contract vehicle for security auditing services.

Contract Personnel

Assura has assigned our most experienced resources to oversee this contract and the services provided. Our leadership will select the best resources available for the services requested based upon their experience and industry certifications. This ensures that our clients have an outstanding service experience with us and that we consistently meet our commitments – on time and on budget.

The following section details the leadership permanently assigned to this contract that is available to JMU and VASCUPP member organizations. Full resumes for these professionals are available upon request.



Karen Cole, CEO

Karen Cole is the co-founder and CEO of Assura, Inc. She has over 20 years of information technology Governance, Risk, and Compliance; and leadership experience.

Her specific areas of expertise are:

- Information Security
- IT Governance
- Enterprise Risk Management
- Business Continuity and Disaster Recovery
- IT Audit and Compliance

For all engagements under this contract, she will be accountable executive and the primary point-of-contact.

Industry Certifications:

- Certified Information Systems Auditor (CISA)
- Certified Business Continuity Planner (CBCP)
- Certified in Risk and Information Systems Control (CRISC)
- Member – Business Continuity Institute (MBCI)

Joshua Cole, Chief Technical Officer

Josh Cole is the Chief Technology Officer and Principal Consultant with Assura, Inc. He has over 25 years of information security and leadership experience.

His specific areas of expertise are:

- Information Security
- IT Governance
- Enterprise Risk Management
- Business Continuity and Disaster Recovery
- Compliance

He will oversee:

- Project Oversight
- Penetration Testing
- Security Engineering and Solutions
- Security Operations Center Oversight

Industry Certifications:

- Certified Information Systems Manager (CISM)

John Brightly, Principal-In-Charge of Client Engagements

John Brightly is a Principal Consultant with Assura, Inc. He has over 25 years of information security and leadership experience.

His specific areas of expertise are:

- Information Security Policy Development, Implementation, and Operationalization
- IT Governance
- Compliance
- Business Continuity and Disaster Recovery

He will oversee:

- Program Development
- Security Assessments

Industry Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Manager (CISM)
- Certified Business Continuity Planner (CBCP)

5. Offeror Data Sheet

ATTACHMENT A
OFFEROR DATA SHEET
TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years 12 Months 6

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
REDACTED	1 Year	REDACTED	REDACTED
REDACTED	5 Years	REDACTED	REDACTED
REDACTED	1.5 Years	REDACTED	REDACTED
REDACTED	8 Years	REDACTED	REDACTED
REDACTED	2 Years	REDACTED	REDACTED

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

   7814 Carousel Lane, Suite 202, Richmond, VA 23294

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [✕] NO
   IF YES, EXPLAIN:_____

6. Small Business Contracting Plan

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: Assura, Inc. _ Prepare Name: Karen L. Cole, CEO

Date: October 24, 2019

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____

If yes, certification number: 661749 Certification date: 7-8-2016

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____

If yes, certification number: 661749 Certification date: 7-8-2016

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No X

If yes, certification number: _____ Certification date: _____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____ If yes, certification number: 661749 Certification date: 7-8-2016

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: Information Technology (IT) Security Auditing Services

Date Form Completed: October 24, 2019

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses for this Proposal and Subsequent Contract

Offeror / Proposer:

Assura, Inc. (Firm) | 7814 Carousel Lane, Suite 202, Richmond, VA 23294 (Address) | Karen L. Cole/804-767-4521 (Contact Person/No.)

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to Date (to be submitted with request for payment from JMU)
Not Applicable as Assura is SWaM certified.	N/A	N/A	N/A	N/A	N/A

(Form shall be submitted with proposal and if awarded, again with submission of each request for payment)

RETURN OF THIS PAGE IS REQUIRED

7. VASCUPP Sales

REDACTED.

Organization	Sales Revenue
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED

8. Proposed Cost

Listed below is the starting hourly rate for each labor category broken. Assura offers substantial discounts from these rates depending on the scope and size of the project, and early payment terms.

Labor Category	MSRP Rate	Discount	Starting Discounted Rate
Principal Consultant	$250.14	5.00%	$237.63
Senior Consultant	$214.64	5.00%	$203.91
Senior Supervisor	$188.86	5.00%	$179.42
Supervisor	$163.11	5.00%	$154.95
Analyst I	$85.86	5.00%	$81.57
Analyst II	$120.18	5.00%	$114.17
Analyst III	$137.36	5.00%	$130.49
Analyst IV	$154.54	5.00%	$146.81
Analyst V	$171.71	5.00%	$163.12
Auditor I	$85.86	5.00%	$81.57
Auditor II	$103.04	5.00%	$97.89
Auditor III	$120.18	5.00%	$114.17
Auditor IV	$137.36	5.00%	$130.49
Auditor V	$154.54	5.00%	$146.81
Security Engineer I	$128.79	5.00%	$122.35
Security Engineer II	$154.54	5.00%	$146.81
Security Engineer III	$188.86	5.00%	$179.42
Project Manager I	$85.86	5.00%	$81.57
Project Manager II	$103.04	5.00%	$97.89
Project Manager III	$120.18	5.00%	$114.17

Please Note: Clients can also request that these services be provided as a fixed-fee project with deliverables billed upon completion of milestones.

9. Additional Information

Although this was not specifically requested in the RFP, Assura submits the following service for consideration. Endpoint devices represent a significant threat vector in an organization. To appropriately identify and remediate risks, regular risk assessments for workstation and mobile devices should be performed.

Endpoint (Workstation and Mobile Device) Risk Assessments

The Assura approach to assessing endpoint security configurations is to scan test targets with the prototype configuration images that are being evaluated. The team will use a combination of tools such as Nessus to both identify vulnerabilities and audit the configurations to ensure compliance with client policies and standards.

Other means that the Assura Team uses to garner security configuration settings are:

- Using the **gpresult /v** command to dump group policy settings;
- Exporting the local security policy from **secpol.msc**; and
- Scan test targets to ensure that their configuration is in alignment with configuration policies deployed by the client's Enterprise Mobility Management (EMM) platform.

The team will use the information obtained from this data gathering to analyze the configurations to ensure that they not only follow client policies and standards but that they also incorporate best practices such as Center for Internet Security (CIS) benchmarks.

The team will ensure that malware prevention/detection and other endpoint security software such as host-based intrusion prevention systems, host-based firewalls are:

- Up-to-date with the latest software versions;
- Configured to automatically download updated signature files; and
- Configured properly to report known and potentially malicious activity.

Based on the results of this effort, the Assura Team will deliver a report that details:

- The security requirements (e.g., compliance with policy, standard, or baseline) and the result of the team's assessment.
- Recommendations for additional controls or settings to enhance security and augment the baseline.

This effort will provide the client with the information it needs to ensure that secure workstation and mobile device configurations are deployed to users and present the lowest possible attack surface to malicious organizations and individuals.

JAMES MADISON UNIVERSITY

Request for Proposal

RFP# FDC-1057

Information Technology (IT)
Security Auditing Services

September 19, 2019

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

REQUEST FOR PROPOSAL
RFP# FDC-1057

Issue Date: **September 19, 2019**

Title: **Information Technology (IT) Security Auditing Services**

Issuing Agency: **Commonwealth of Virginia**
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on October 17, 2019 for Furnishing The Services Described Herein.

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.
In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature in Ink)

Name: _____
(Please Print)

Date: _____ Title: _____

Web Address: _____ Phone: _____

Email: _____ Fax #: _____

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1_____ #2_____ #3_____ #4_____ #5_____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
□ YES; □ NO; ***IF YES*** ⇒⇒ □ SMALL; □ WOMAN; □ MINORITY ***IF MINORITY***: □ AA; □ HA; □ AsA; □ NW; □ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

REQUEST FOR PROPOSAL

RFP # FDC-1057

TABLE OF CONTENTS

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals from qualified sources to enter into a contract to provide **Information Technology (IT) Security Auditing Services** for James Madison University (JMU), an agency of the Commonwealth of Virginia. Initial contract shall be for one (1) year with an option to renew for four (4) additional one-year periods.

II. BACKGROUND

James Madison University (JMU) is a comprehensive public institution in Harrisonburg, Virginia with an enrollment of approximately 21,000 students and 3,000 faculty and staff. There are over 600 individual departments on campus that support seven academic divisions. The University offers over 120 majors, minors, and concentrations. Further information about the University may be found at the following website: http://www.jmu.edu.

The objective of James Madison University's Audit Management Services Department is to provide reasonable assurance to management, within reasonable economic limitations, that:

A. Internal accounting controls are adequate and effective in promoting efficiency and in protecting the assets of the University.
B. Financial statement and reports, whether for internal or external use, comply with established policies, generally accepted accounting principles, and/or other applicable rules and regulations both State and Federal.
C. Operational policies promote the well-being of the University and are effective and enforced to the end that operational efficiency and effectiveness are achieved.
D. Adequate standards of business conduct are being observed.
E. Internal control over information security activities, either internal or as provided by the fiscal agent and other contractors, is sufficient to reasonably ensure efficient, accurate, and complete processing of University data with due regard to security.
F. Contractors who are providing services to the University are doing so in a manner in accordance with all contract provisions.
G. Contractor billings conform to the predetermined formats and contain sufficient information to fully support University evaluation and payment.
H. University data in the hands of contractors is maintained in a secure and efficient manner according to formal backup, disaster and data recovery plans.

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

It is the policy of the Commonwealth of Virginia to contribute to the establishment, preservation, and strengthening of small businesses and businesses owned by women and minorities, and to encourage their participation in State procurement activities. The Commonwealth encourages contractors to provide for the participation of small businesses and businesses owned by women and minorities through partnerships, joint ventures, subcontracts, and other contractual opportunities. Attachment B contains information on reporting spend data with subcontractors.

IV. STATEMENT OF NEEDS

A. James Madison University desires to contract with qualified firms to provide expertise and a range of services to support technologies used by the University. Contractor shall serve on special projects as a technology expert when requested and as needed. Reports shall be provided back to the University summarizing options and providing recommendations.

Contractor shall serve as a technology advisor to understand, communicate, and propose solutions as requested. Contractor shall serve as a resource of research, implementation, troubleshooting, and other technical tasks to support the efforts of James Madison University Information Technology (JMU IT) staff. Functional consultants shall be represented by the Contractor as experts in the tasks and functions assigned. The University reserves the right to accept or reject any proposed or assigned consultant, without cause, at any time during the duration of the contract.

B. The selected contractor(s) shall supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit and Management Services. James Madison University does not guarantee any work being assigned to the selected contractor(s). If multiple awards are issued as a result of this solicitation, JMU reserves the right to select the contractor who in their sole opinion is best suited for each particular project on a project by project basis.

C. The University's Audit and Management Services (AMS) requires, at a minimum, the following supplemental support for its IT auditing functions:

1. Describe your company's plan to provide certified professional staff to perform a wide range of IT audits of various IT activities and processes under the direction of the Director or staff of AMS. The list below are audits currently performed by University personnel or by the staff of contractors performing under formal statement of work agreements with the University.*

    a. External Vulnerability Scanning
    b. Wireless Network Assessment
    c. Firewall and Router Security Assessment
    d. Server Configurations Assessment
    e. Database Architecture Security Assessment
    f. Network Scanning Process Assessment
    g. Web Application Security Assessments
    h. Active Directory Security Assessment
    i. Penetration Testing
    j. Telecommunications

    **Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP).*

2. Describe your company's past history in working with any institutions of higher education, especially those within the Commonwealth of Virginia.

Specific scope requirements and deliverables will be included in an individual statement of work (SOW) for each separate project.

D. Billing Rate:

The Offeror shall provide an hourly rate broken down by position type for the proposed services. Provide onsite hourly rate that includes all billables (e.g. travel, lodging, etc.). Include pricing for all other products and services. Please see section X. PRICING SCHEDULE

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

To ensure timely and adequate consideration of your proposal, offerors are to limit all contact, whether verbal or written, pertaining to this RFP to the James Madison University Procurement Office for the duration of this Proposal process. Failure to do so may jeopardize further consideration of Offeror's proposal.

1. RFP Response: In order to be considered for selection, the **Offeror shall submit a complete response to this RFP**; and shall submit to the issuing Purchasing Agency:

   a. **One (1) original** and **four (4) copies** of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f. below.

   b. **One (1) electronic copy in WORD format or searchable PDF** (*CD or flash drive*) of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f. below.

   c. Should the proposal contain **proprietary information**, provide **one (1) redacted hard copy** of the proposal and all attachments with **proprietary portions removed or blacked out**. This copy should be clearly marked "*Redacted Copy*" on the front cover. The classification of an entire proposal document, line item prices, and/or total proposal prices as proprietary or trade secrets is not acceptable. JMU shall not be responsible for the Contractor's failure to exclude proprietary information form this redacted copy.

   No other distribution of the proposal shall be made by the Offeror.

2. The version of the solicitation issued by JMU Procurement Services, as amended by an addenda, is the mandatory controlling version of the document. Any modification of, or additions to, the solicitation by the Offeror shall not modify the official version of the solicitation issued by JMU Procurement services unless accepted in writing by the University. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, JMU reserves the right to decide, on a case-by-case basis in its sole discretion, whether to reject such a proposal. If the modification or additions are not identified until after the award of the contract, the controlling version of the solicitation document shall still be the official state form issued by Procurement Services.

3. Proposal Preparation

   a. Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested

may result in the purchasing agency requiring prompt submissions of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

b. Proposals shall be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and sub letter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at the appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

d. As used in this RFP, the terms "must", "shall", "should" and "may" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the proposed solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have a large impact and would be useful, but are not necessary. Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of an offeror to satisfy a "must" or "shall" requirement does not automatically remove that offeror from consideration; however, it may seriously affect the overall rating of the offeror' proposal.

e. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.

f. Ownership of all data, materials and documentation originated and prepared for the State pursuant to the RFP shall belong exclusively to the State and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by the offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the offeror must invoke the protection of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data is submitted. The written notice must specifically identify the data or materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret materials submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and will result in rejection and return of the proposal.

4. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to James Madison University. This provides an opportunity for the Offeror to clarify or elaborate on the proposal. This is a fact-finding and explanation session only and does not include negotiation. James Madison University will schedule the time and location of these presentations. Oral presentations are an option of the University and may or may not be conducted. Therefore, proposals should be complete.

B. SPECIFIC PROPOSAL INSTRUCTIONS

Proposals should be as thorough and detailed as possible so that James Madison University may properly evaluate your capabilities to provide the required services. Offerors are required to submit the following items as a complete proposal:

1. Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required.

2. Plan and methodology for providing the goods/services as described in Section IV. Statement of Needs of this Request for Proposal.

3. A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

4. Offeror Data Sheet, included as *Attachment A* to this RFP.

5. Small Business Subcontracting Plan, included as *Attachment B* to this RFP. Offeror shall provide a Small Business Subcontracting plan which summarizes the planned utilization of Department of Small Business and Supplier Diversity (SBSD)-certified small businesses which include businesses owned by women and minorities, when they have received Department of Small Business and Supplier Diversity (SBSD) small business certification, under the contract to be awarded as a result of this solicitation. This is a requirement for all prime contracts in excess of $100,000 unless no subcontracting opportunities exist.

6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org.

7. Proposed Cost. See Section X. Pricing Schedule of this Request for Proposal.

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

Proposals shall be evaluated by James Madison University using the following criteria:

	Points
1. Quality of products/services offered and suitability for intended purposes	25
2. Qualifications and experience of Offeror in providing the goods/services	25

3.	Specific plans or methodology to be used to perform the services	20
4.	Participation of Small, Women-Owned, & Minority (SWaM) Businesses	10
5.	Cost	20
		100

B. AWARD TO MULTIPLE OFFERORS: Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposals, including price, if so stated in the Request for Proposals. Negotiations shall be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each offeror so selected, the agency shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. The Commonwealth reserves the right to make multiple awards as a result of this solicitation. The Commonwealth may cancel this Request for Proposals or reject proposals at any time prior to an award, and is not required to furnish a statement of the reasons why a particular proposal was not deemed to be the most advantageous. Should the Commonwealth determine in writing and in its sole discretion that only one offeror is fully qualified, or that one offeror is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of the solicitation and the contractor's proposal as negotiated.

VII. GENERAL TERMS AND CONDITIONS

A. PURCHASING MANUAL: This solicitation is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. A copy of the manual is available for review at the purchasing office. In addition, the manual may be accessed electronically at http://www.jmu.edu/procurement or a copy can be obtained by calling Procurement Services at (540) 568-3145.

B. APPLICABLE LAWS AND COURTS: This solicitation and any resulting contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with applicable federal, state and local laws and regulations.

C. ANTI-DISCRIMINATION: By submitting their proposals, offerors certify to the Commonwealth that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and §10 of the Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 (available for review at http://www.jmu.edu/procurement). If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. *(§6 of the Rules Governing Procurement*).

In every contract over $10,000 the provisions in 1. and 2. below apply:

1. During the performance of this contract, the contractor agrees as follows:

   a. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the contractor. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

   b. The contractor, in all solicitations or advertisements for employees placed by or on behalf of the contractor, will state that such contractor is an equal opportunity employer.

   c. Notices, advertisements, and solicitations placed in accordance with federal law, rule, or regulation shall be deemed sufficient for the purpose of meeting these requirements.

2. The contractor will include the provisions of 1. Above in every subcontract or purchase order over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

D. ETHICS IN PUBLIC CONTRACTING: By submitting their proposals, offerors certify that their proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other offeror, supplier, manufacturer or subcontractor in connection with their proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

E. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By entering into a written contract with the Commonwealth of Virginia, the Contractor certifies that the Contractor does not, and shall not during the performance of the contract for goods and services in the Commonwealth, knowingly employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

F. DEBARMENT STATUS: By submitting their proposals, offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred.

G. ANTITRUST: By entering into a contract, the contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

H. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS RFPs: Failure to submit a proposal on the official state form provided for that purpose may be a cause for rejection of the proposal. Modification of or additions to the General Terms and Conditions of the solicitation may be cause for rejection of the proposal; however, the Commonwealth

reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal.

I. CLARIFICATION OF TERMS: If any prospective offeror has questions about the specifications or other solicitation documents, the prospective offeror should contact the buyer whose name appears on the face of the solicitation no later than five working days before the due date. Any revisions to the solicitation will be made only by addendum issued by the buyer.

J. PAYMENT:

1. To Prime Contractor:

a. Invoices for items ordered, delivered and accepted shall be submitted by the contractor directly to the payment address shown on the purchase order/contract. All invoices shall show the state contract number and/or purchase order number; social security number (for individual contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

b. Any payment terms requiring payment in less than 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 30 days, however.

c. All goods or services provided under this contract or purchase order, that are to be paid for with public funds, shall be billed by the contractor at the contract price, regardless of which public agency is being billed.

d. The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

e. Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, the Commonwealth shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this section do not relieve an agency of its prompt payment obligations with respect to those charges which are not in dispute (*Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 § 53; available for review at http://www.jmu.edu/procurement*).

2. To Subcontractors:

a. A contractor awarded a contract under this solicitation is hereby obligated:

(1) To pay the subcontractor(s) within seven (7) days of the contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractor(s) under the contract; or

(2) To notify the agency and the subcontractors, in writing, of the contractor's intention to withhold payment and the reason.

b. The contractor is obligated to pay the subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the contractor that remain unpaid seven (7) days following receipt of payment from the Commonwealth, except for amounts withheld as stated in (2) above. The date of mailing of any payment by U. S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier contractor performing under the primary contract. A contractor's obligation to pay an interest charge to a subcontractor may not be construed to be an obligation of the Commonwealth.

3. Each prime contractor who wins an award in which provision of a SWAM procurement plan is a condition to the award, shall deliver to the contracting agency or institution, on or before request for final payment, evidence and certification of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the SWAM procurement plan. Final payment under the contract in question may be withheld until such certification is delivered and, if necessary, confirmed by the agency or institution, or other appropriate penalties may be assessed in lieu of withholding such payment.

4. The Commonwealth of Virginia encourages contractors and subcontractors to accept electronic and credit card payments.

K. PRECENDENCE OF TERMS: Paragraphs A through J of these General Terms and Conditions and the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors, shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

L. QUALIFICATIONS OF OFFERORS: The Commonwealth may make such reasonable investigations as deemed proper and necessary to determine the ability of the offeror to perform the services/furnish the goods and the offeror shall furnish to the Commonwealth all such information and data for this purpose as may be requested. The Commonwealth reserves the right to inspect offeror's physical facilities prior to award to satisfy questions regarding the offeror's capabilities. The Commonwealth further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such offeror fails to satisfy the Commonwealth that such offeror is properly qualified to carry out the obligations of the contract and to provide the services and/or furnish the goods contemplated therein.

M. TESTING AND INSPECTION: The Commonwealth reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.

N. ASSIGNMENT OF CONTRACT: A contract shall not be assignable by the contractor in whole or in part without the written consent of the Commonwealth.

O. CHANGES TO THE CONTRACT: Changes can be made to the contract in any of the following ways:

1. The parties may agree in writing to modify the scope of the contract. An increase or decrease in the price of the contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the contract.

2. The Purchasing Agency may order changes within the general scope of the contract at any time by written notice to the contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The contractor shall comply with the notice upon receipt. The contractor shall be compensated for any additional costs incurred as the result of such order and shall give the Purchasing Agency a credit for any savings. Said compensation shall be determined by one of the following methods:

    a. By mutual agreement between the parties in writing; or

    b. By agreeing upon a unit price or using a unit price set forth in the contract, if the work to be done can be expressed in units, and the contractor accounts for the number of units of work performed, subject to the Purchasing Agency's right to audit the contractor's records and/or to determine the correct number of units independently; or

    c. By ordering the contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The contractor shall present the Purchasing Agency with all vouchers and records of expenses incurred and savings realized. The Purchasing Agency shall have the right to audit the records of the contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to the Purchasing Agency within thirty (30) days from the date of receipt of the written order from the Purchasing Agency. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors. Neither the existence of a claim nor a dispute resolution process, litigation or any other provision of this contract shall excuse the contractor from promptly complying with the changes ordered by the Purchasing Agency or with the performance of the contract generally.

P. DEFAULT: In case of failure to deliver goods or services in accordance with the contract terms and conditions, the Commonwealth, after due oral or written notice, may procure them from other sources and hold the contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which the Commonwealth may have.

Q. INSURANCE: By signing and submitting a proposal under this solicitation, the offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the contract is awarded. For construction contracts, if any subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with§ 25 of the Rules Governing Procurement – Chapter 2, Exhibit J, Attachment 1, and 65.2-800 et. Seq. of the Code of Virginia (available for review at http://www.jmu.edu/procurement) The offeror further certifies that the contractor and any subcontractors will maintain these insurance coverage during the entire term of the contract and that all insurance coverage will be provided

by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

1. Workers' Compensation: Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify the Commonwealth of increases in the number of employees that change their workers' compensation requirement under the Code of Virginia during the course of the contract shall be in noncompliance with the contract.

2. Employer's Liability: $100,000

3. Commercial General Liability: $1,000,000 per occurrence and $2,000,000 in the aggregate. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. The Commonwealth of Virginia must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability: $1,000,000 combined single limit. (*Required only if a motor vehicle not owned by the Commonwealth is to be used in the contract. Contractor must assure that the required coverage is maintained by the Contractor (or third party owner of such motor vehicle.*)

R. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract over $100,000, as a result of this solicitation, the purchasing agency will publicly post such notice on the DGS/DPS eVA web site (www.eva.virginia.gov) for a minimum of 10 days.

S. DRUG-FREE WORKPLACE: During the performance of this contract, the contractor agrees to (i) provide a drug-free workplace for the contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the contractor that the contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

For the purposes of this section, "drug-free workplace" means a site for the performance of work done in connection with a specific contract awarded to a contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the contract.

T. NONDISCRIMINATION OF CONTRACTORS: An offeror, or contractor shall not be discriminated against in the solicitation or award of this contract because of race, religion, color, sex, national origin, age, disability, faith-based organizational status, any other basis prohibited by state law relating to discrimination in employment or because the offeror employs ex-offenders unless the state agency, department or institution has made a written determination that employing ex-offenders on the specific contract is not in its best interest. If the award of this contract is made to a faith-based organization and an individual, who applies

for or receives goods, services, or disbursements provided pursuant to this contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

U. eVA BUSINESS TO GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal www.eVA.virginia.gov, streamlines and automates government purchasing activities in the Commonwealth. The eVA portal is the gateway for vendors to conduct business with state agencies and public bodies. All vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet eprocurement solution by completing the free eVA Vendor Registration. All offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the proposal being rejected. Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:

   a. Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $500 per order.

   b. Businesses that are not Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $1,500 per order.

2. For orders issued prior to July 1, 2014 the vendor transaction fees can be found at www.eVA.virginia.gov.

3. The specified vendor transaction fee will be invoiced by the Commonwealth of Virginia Department of General Services approximately 60 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

V. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the Commonwealth of Virginia shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

W. PRICING CURRENCY: Unless stated otherwise in the solicitation, offerors shall state offered prices in U.S. dollars.

X. E-VERIFY REQUIREMENT OF ANY CONTRACTOR: 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 James Madison University 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 any awarded contract.

VIII. SPECIAL TERMS AND CONDITIONS

A. AUDIT: The Contractor hereby agrees to retain all books, records, systems, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The Commonwealth of Virginia, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

B. CANCELLATION OF CONTRACT: James Madison University reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

C. IDENTIFICATION OF PROPOSAL ENVELOPE: The signed proposal should be returned in a separate envelope or package, sealed and identified as follows:

From: _____

Name of Offeror | Due Date | Time

Street or Box No. | RFP #

City, State, Zip Code | RFP Title

Name of Purchasing Officer:

The envelope should be addressed as directed on the title page of the solicitation.

The Offeror takes the risk that if the envelope is not marked as described above, it may be inadvertently opened and the information compromised, which may cause the proposal to be disqualified. Proposals may be hand-delivered to the designated location in the office issuing the solicitation. No other correspondence or other proposals should be placed in the envelope.

D. LATE PROPOSALS: To be considered for selection, proposals must be received by the issuing office by the designated date and hour. The official time used in the receipt of proposals is that time on the automatic time stamp machine in the issuing office. Proposals received in the issuing office after the date and hour designated are automatically non responsive and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intra university mail system. It is the sole responsibility of the Offeror to ensure that its proposal reaches the issuing office by the designated date and hour.

E. UNDERSTANDING OF REQUIREMENTS: It is the responsibility of each offeror to inquire about and clarify any requirements of this solicitation that is not understood. The University will not be bound by oral explanations as to the meaning of specifications or language contained in this solicitation. Therefore, all inquiries deemed to be substantive in nature must be in writing and submitted to the responsible buyer in the Procurement Services Office. Offerors must ensure that written inquiries reach the buyer at least five (5) days prior to the time set for receipt of offerors proposals. A copy of all queries and the respective response will be provided in the form of an addendum to all offerors who have indicated an interest in responding to this

solicitation. Your signature on your Offer certifies that you fully understand all facets of this solicitation. These questions may be sent by Fax to 540/568-7935.

F. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for a period of four (4) successive one year periods under the terms and conditions of the original contract except as stated in 1. and 2. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew shall be given approximately 90 days prior to the expiration date of each contract period.

1. If the Commonwealth elects to exercise the option to renew the contract for an additional one-year period, the contract price(s) for the additional one year shall not exceed the contract price(s) of the original contract increased/decreased by no more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

2. If during any subsequent renewal periods, the Commonwealth elects to exercise the option to renew the contract, the contract price(s) for the subsequent renewal period shall not exceed the contract price(s) of the previous renewal period increased/decreased by more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

G. SUBMISSION OF INVOICES: All invoices shall be submitted within sixty days of contract term expiration for the initial contract period as well as for each subsequent contract renewal period. Any invoices submitted after the sixty day period will not be processed for payment.

H. OPERATING VEHICLES ON JAMES MADISON UNIVERSITY CAMPUS: Operating vehicles on sidewalks, plazas, and areas heavily used by pedestrians is prohibited. In the unlikely event a driver should find it necessary to drive on James Madison University sidewalks, plazas, and areas heavily used by pedestrians, the driver must yield to pedestrians. For a complete list of parking regulations, please go to www.jmu.edu/parking; or to acquire a service representative parking permit, contact Parking Services at 540.568.3300. The safety of our students, faculty and staff is of paramount importance to us. Accordingly, violators may be charged.

I. COOPERATIVE PURCHASING / USE OF AGREEMENT BY THIRD PARTIES: It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations may access any resulting contract if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the entities indicated above to purchase goods and services in accordance with contract terms. As a separate contractual relationship, the participating entity will place its own orders directly with the Contractor(s) and shall fully and independently administer its use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the University. No modification of this contract or execution of a separate agreement is required to participate; however, the participating entity and the Contractor may modify the terms and conditions of this contract to accommodate specific governing laws, regulations, policies, and business goals

required by the participating entity. Any such modification will apply solely between the participating entity and the Contractor.

The Contractor will notify the University in writing of any such entities accessing this contract. The Contractor will provide semi-annual usage reports for all entities accessing the contract. The University shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the University is not responsible for the acts or omissions of any entity and will not be considered in default of the contract no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes as needed.

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

1. It is the goal of the Commonwealth that 42% of its purchases are made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All potential offerors are required to submit a Small Business Subcontracting Plan. Unless the offeror is registered as a Department of Small Business and Supplier Diversity (SBSD)-certified small business and where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such subcontracting opportunities to SBSD-certified small businesses. This shall not exclude SBSD-certified women-owned and minority-owned businesses when they have received SBSD small business certification. No offeror or subcontractor shall be considered a Small Business, a Women-Owned Business or a Minority-Owned Business unless certified as such by the Department of Small Business and Supplier Diversity (SBSD) by the due date for receipt of proposals. If small business subcontractors are used, the prime contractor agrees to report the use of small business subcontractors by providing the purchasing office at a minimum the following information: name of small business with the SBSD certification number or FEIN, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product/service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807.**

2. Each prime contractor who wins an award in which provision of a small business subcontracting plan is a condition of the award, shall deliver to the contracting agency or institution with every request for payment, evidence of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the small business subcontracting plan. **This information shall be submitted to: JMU Office of Procurement Services, SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807**. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm with the Department of Small Business and Supplier Diversity (SBSD) certification number or FEIN number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product or service provided. Payment(s) may be withheld until compliance with the plan is received and confirmed by the agency or institution. The agency or institution reserves the right to pursue other appropriate remedies to include, but not be limited to, termination for default.

3. Each prime contractor who wins an award valued over $200,000 shall deliver to the contracting agency or institution with every request for payment, information on use of subcontractors that are not Department of Small Business and Supplier Diversity (SBSD)-

certified small businesses. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, FEIN number, total dollar amount subcontracted, and type of product or service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807**.

K. ADDITIONAL GOODS AND SERVICES: The University may acquire other goods or services that the supplier provides than those specifically solicited. The University reserves the right, subject to mutual agreement, for the Contractor to provide additional goods and/or services under the same pricing, terms, and conditions and to make modifications or enhancements to the existing goods and services. Such additional goods and services may include other products, components, accessories, subsystems, or related services that are newly introduced during the term of this Agreement. Such additional goods and services will be provided to the University at favored nations pricing, terms, and conditions.

L. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH: A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a registered limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the Code of Virginia or as otherwise required by law. Any business entity described above that enters into a contract with a public body shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section.

M. PUBLIC POSTING OF COOPERATIVE CONTRACTS: James Madison University maintains a web-based contracts database with a public gateway access. Any resulting cooperative contract/s to this solicitation will be posted to the publicly accessible website. Contents identified as proprietary information will not be made public.

N. CRIMINAL BACKGROUND CHECKS OF PERSONNEL ASSIGNED BY CONTRACTOR TO PERFORM WORK ON JMU PROPERTY: The Contractor shall obtain criminal background checks on all of their contracted employees who will be assigned to perform services on James Madison University property. The results of the background checks will be directed solely to the Contractor. The Contractor bears responsibility for confirming to the University contract administrator that the background checks have been completed prior to work being performed by their employees or subcontractors. The Contractor shall only assign to work on the University campus those individuals whom it deems qualified and permissible based on the results of completed background checks. Notwithstanding any other provision herein, and to ensure the safety of students, faculty, staff and facilities, James Madison University reserves the right to approve or disapprove any contract employee that will work on JMU property. Disapproval by the University will solely apply to JMU property and should have no bearing on the Contractor's employment of an individual outside of James Madison University.

O. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the contractor/any services of any kind or nature furnished by the contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use

the materials, goods, or equipment in the manner already and permanently described by the contractor on the materials, goods or equipment delivered.

P. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to James Madison University will be used in product literature or advertising without the express written consent of the University. The contractor shall not state in any of its advertising or product literature that James Madison University has purchased or uses any of its products or services, and the contractor shall not include James Madison University in any client list in advertising and promotional materials without the express written consent of the University.

Q. PRIME CONTRACTOR RESPONSIBILITIES: The contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime contractor. The contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

R. SUBCONTRACTS: No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the contractor desires to subcontract some part of the work specified herein, the contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.

S. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The contractor assures that information and data obtained as to personal facts and circumstances related to faculty, staff, students, and affiliates will be collected and held confidential, during and following the term of this agreement, and will not be divulged without the individual's and the agency's written consent and only in accordance with federal law or the Code of Virginia. *This shall include FTI, which is a term of art and consists of federal tax returns and return information (and information derived from it) that is in contractor/agency possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as sensitive but unclassified information and may contain personally identifiable information (PII).* Contractors who utilize, access, or store personally identifiable information as part of the performance of a contract are required to safeguard this information and immediately notify the agency of any breach or suspected breach in the security of such information. Contractors shall allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting. Contractors and their employees working on this project may be required to sign a confidentiality statement.

IX. METHOD OF PAYMENT

The contractor will be paid on the basis of invoices submitted in accordance with the solicitation and any negotiations. James Madison University recognizes the importance of expediting the payment process for our vendors and suppliers. We are asking our vendors and suppliers to enroll in the Wells Fargo Bank single use Commercial Card Number process or electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the Wells Fargo Bank single use Commercial Card Number process will receive the benefit of being paid in Net 15 days. Additional information is available online at: http://www.jmu.edu/financeoffice/accounting-operations-disbursements/cash-investments/vendor-payment-methods.shtml

X. PRICING SCHEDULE

The Offeror shall provide an hourly rate broken down by position type for the proposed services. For each of the rates also provide an onsite hourly rate that includes all billables (e.g. travel, lodging, etc.). Include pricing for all other products and services. The resulting contract will be cooperative and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2.

Specify any associated charge card processing fees, if applicable, to be billed to the university. Vendors shall provide their VISA registration number when indicating charge card processing fees. Any vendor requiring information on VISA registration may refer to https://usa.visa.com/support/small-business/regulations-fees.html and for questions https://usa.visa.com/dam/VCOM/global/support-legal/documents/merchant-surcharging-qa-for-web.pdf.

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

Attachment B: Small, Women, and Minority-owned Business (SWaM) Utilization Plan

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years_____ Months_____

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

_____

_____

_____

_____

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [ ] NO
   IF YES, EXPLAIN:_____

_____

_____

_____

ATTACHMENT B

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: _____ Preparer Name: _____

Date: _____

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date: _____

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: _____ Date Form Completed:_____

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses
for this Proposal and Subsequent Contract

Offeror / Proposer:

_____	_____	_____
Firm	Address	Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)

(Form shall be submitted with proposal and if awarded, again with submission of each request for payment)

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

This contract entered into this_____day of_____20____,by _____ hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

WITNESSETH that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposals dated _____:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) List each addendum that may be issued

(3) The Contractor's Proposal dated _____and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations summary dated _____.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By:_____	By:_____
(Signature)	(Signature)
_____	_____
(Printed Name)	(Printed Name)
Title:_____	Title:_____

ATTACHMENT D

Zone Map

Virginia Association of State College & University Purchasing Professionals (VASCUPP)

List of member institutions by zones

Zone 1	**Zone 2**	**Zone 3**
George Mason University (Fairfax)	James Madison University (Harrisonburg)	University of Virginia (Charlottesville)
Zone 4	**Zone 5**	**Zone 6**
University of Mary Washington (Fredericksburg)	College of William and Mary (Williamsburg) Old Dominion University (Norfolk)	Virginia Commonwealth University (Richmond)
Zone 7	**Zone 8**	**Zone 9**
Longwood University (Farmville)	Virginia Military Institute (Lexington) Virginia Tech (Blacksburg) Radford University (Radford)	University of Virginia - Wise (Wise)

JAMES MADISON UNIVERSITY

October 9, 2019

ADDENDUM NO.: One

TO ALL OFFERORS:

REFERENCE:	Request for Proposal No:	**RFP# FDC-1057**
	Dated:	September 19, 2019
	Commodity:	Information Technology (IT) Security Auditing Services
	RFP Closing On:	~~October 17, 2019 @ 2:00 pm.~~ **October 24, 2019 @ 2:00 pm**

Please note the clarifications and/or changes made on this proposal program:

The closing date/time has been extended until October 24, 2019, at 2:00 pm EST.

1. Question: Does JMU have current providers for these services, and if so, who?

   Answer: Telasa Security, LLC and Syrinx Technologies, LLC are the current providers for these services.

2. Question: Section V. B. 6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org. Is this item a requirement in order to submit a proposal?

   Answer: Please provide an answer to this question. Previous work with VASCUPP Member Institutions is not a requirement to be consider for award.

3. Question: Do you expect the work to be done on and off-site or on-site only?

   Answer: Depending upon the project, the work may be done entirely off-site, or may require on-site testing with off-site report writing and follow-up. Please provide an hourly rate for off-site work, and an hourly rate for on-site work including all billables, as noted in X. Pricing Schedule.

   "The Offeror shall provide an hourly rate broken down by position type for the proposed services. For each of the rates also provide an onsite hourly rate that includes all billables (e.g. travel, lodging, etc.). Include pricing for all other products and services. The resulting contract will be cooperative and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2."

4. Question: Are there other locations involved than Harrisonburg, VA and is any travel involved.

   Answer: The only location is in Harrisonburg, VA. Also, please see the answer to the previous question.

5. Question: In regards to the Small Business, MWBE goal, it there one?

   Answer: No specific SWaM goal has been established for this solicitation and potential resulting contract. However, the University has SWaM goals that encourage use of the use of small, women, and minority vendors whenever possible and practical.

MSC 5720
752 Ott Street, Room 1042
Wine Price Building
Harrisonburg, VA 22807
Office of 540.568.3145 Phone
PROCUREMENT SERVICES 540.568.7936 Fax

6. Question: Are there specific numbers of FTEs needed for each requirement?

   Answer: The number of FTEs could vary for each project, however, most projects can be done by one person if they have the expertise.

7. Question: Are there any special formats for resumes and are there any page limitations for submission?

   Answer: There are no specific requirements for resumes that are submitted as part of your proposal response. There are no page limits, but please keep the following in mind when preparing your proposal response submission:

   Section V. A. 3. b. - Proposals shall be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

8. Question: Is there a new project or on-going effort and expected award or start date for the project?

   Answer: The examples of IT audits listed in IV.C.1. are typical audits that are of short duration (two days to two months). Each audit is considered a separate project and may be awarded to a contractor based on a specific statement of work agreement. Projects are scheduled based on the needs of the university, peak system usage times, and contractor availability.

   The potential award date of this contract will depend on the number of responses received, the quality of the responses, the time needed for the committee to evaluate the submissions, JMU upcoming holiday schedule, and the responsiveness of vendors to follow up or negotiation questions.

   The current contract for these services end on 2/23/20. The goal is to have a new contract in place so that there is no gap in services.

9. Question: Does JMU already have infrastructure in place for the specific task that you are looking to achieve or company has to provide the project management and solution as well, beside resources?

   Answer: For each project, the contractor is expected to provide project management for the work agreed upon in the statement of work.

10. Question: The proposal says "multi BPA, project to project basis", please confirm if its multi-vendor award BPA based on assigned task to each company?

    Answer: The contract may be awarded to multiple companies as needed to ensure that we have the expertise to support our audit plan. Each project will be then be contracted separately.

11. Question: Is the use of 1099 permitted?

    Answer: The contractor will be paid in accordance with the statement of work developed for the project. JMU will issue a 1099 to the contractor for the amount paid in the calendar year.

12. Question: How many hours do we expect annually per position and is it M-F 9 to 5 work schedule or as needed?

    Answer: The statement of work for each project will outline the hours expected for that project and the projected timeline of the project.

13. Question: Are you expecting resources only from a biding company to complete the required tasks listed in RFP from A to J or PM and resources both?

    Answer: For each project, a statement of work will be developed with a selected contractor. The contractor will be expected to provide project management, personnel, and any licensed software necessary for the work agreed upon in the statement of work.

14. Question: With regards to section V. B. 6. - Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org. Is this to say total sales using VASCUPP contract or just sales to VASCUPP members regardless of contract vehicle?

    Answer: Total sales regardless of contract vehicle.

15. Question: What is the security framework used for the assessment? Many Institutes of Higher Education (IHE) use a variety of frameworks such as NIST Cybersecurity Framework version 1.1, NIST SP 800-53 or even NIST SP 800-171.

    Answer: JMU follows ISO 27002 for guidance.

16. Question: Do the configurations of networking equipment need to meet specific standards for Compliance?

    Answer: We follow ISO 27002 for guidance along with industry standard best practices.

17. Question: The goal of this assessment seems to be verification of controls which should be in place to protect University data. Are there areas which should be reviewed more closely?

    Answer: The examples of IT audits listed in IV.C.1 are past audits that have been done in the past. An IT risk assessment is performed each year, and a project list is developed based upon the risk assessment.

18. Question: Are all of the areas in the RFP to be covered (sections a-j) in one assessment or would these be performed in separate assessments?

    Answer: Separate assessments – see answer 19 below as well.

19. Question: If we need to estimate the cost below we need the following questions answered:

    a. External Vulnerability Scanning - How many IPs are we scanning?
    b. Wireless Network Assessment - How many access points and number of locations to be included?
    c. Firewall and Router Security Assessment - Can a baseline be provided?
    d. Server Configurations Assessment - Can a baseline be provided?
    e. Database Architecture Security Assessment - falls under pen testing
    f. Network Scanning Process Assessment- Need more clarity here. Is JMU looking for a tool or an evaluation of the current process?
    g. Web Application Security Assessments - falls under pen testing
    h. Active Directory Security Assessment - falls under pen testing
    i. Penetration Testing
    j. Telecommunications - What types of request fall into this category?

    Answer: The overall contract may be awarded to multiple companies as needed to ensure that we have the expertise to support our audit plan. Each project will be then be contracted separately with a selected contractor. A pre-audit conference is conducted to develop the scope of work for each project. The contractor then submits a proposal for the project with an estimate of hours (and total cost) of the project. Approval of the proposal by Audit and Management Services creates the contract for the project.

The examples of IT audits listed in IV.C.1. and below are typical audits that are of short duration (two days to two months). Each audit is considered a separate project and may be awarded to a contractor based on a specific statement of work agreement. Projects are scheduled based on the needs of the university, peak system usage times, and contractor availability. The statement of work for each project will outline scope of the project, the hours expected for that project and the projected timeline of the project. For each project, the statement of work will be developed with input from the selected contractor, IT, and JMU Audit and Management Services. The contractor will be expected to provide project management, personnel, and any licensed software necessary for the work agreed upon in the statement of work.

Depending upon the project, the work may be done entirely off-site, or may require on-site testing with off-site report writing and follow-up. Please provide an hourly rate for off-site work, and an hourly rate for on-site work including all billables, as noted in X. Pricing Schedule.

"The Offeror shall provide an hourly rate broken down by position type for the proposed services. For each of the rates also provide an onsite hourly rate that includes all billables (e.g. travel, lodging, etc.). Include pricing for all other products and services. The resulting contract will be cooperative and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2."

20. Question: What is the security framework used for the assessment? Many Institutes of Higher Education (IHE) use a variety of frameworks such as NIST Cybersecurity Framework version 1.1, NIST SP 800-53 or even NIST SP 800-171.

    Answer: JMU's IT follows ISO 27002 for guidance.

21. Question: Is there a dedicated staff for IT Security?

    Answer: Yes.

22. Question: Regarding access…Internal scans and assessments require interaction with and cooperation with IT staff. Evaluating configurations of security, network, server and endpoint systems requires access to systems, which can only be done through IT.

    Answer: JMU will provide workspace and network connectivity if work is done on-site. The contractor is expected to provide laptops and licensed software needed for testing. JMU's IT will facilitate running of scripts when necessary. When necessary, IT will work with the contractor to open ports, etc. for testing purposes.

23. Question: Will there be information about the environment shared with the team in advance of any automated scans?

    Answer: Yes. A pre-audit conference is always scheduled.

24. Question: Do the configurations of networking equipment need to meet specific standards for Compliance?

    Answer: JMU's IT follows ISO 27002 for guidance, along with industry standard best practices.

25. Question: Do we provide cost for hourly rate for certified staff only for billable requests or do we provide hourly rate with an estimate for each of the audit range items below?

    Answer: We want two hourly rates (on-site, off-site) that could be applied to all the projects. Depending upon the project, the work may be done entirely off-site, or may require on-site testing with off-site report writing and follow-up. Please provide an hourly rate for off-site work, and an hourly rate for on-site work including all billables, as noted in X. Pricing Schedule.

26. Question: Section IV.C.2 of the RFP that vendors should describe our company's past history working with any institutions of higher education. Are you looking for past performance specific to the same services outlined in the RFP, or would any broader IT support services that we have provided to institutions of higher education would be of interest?

    Answer: We are most interested in history regarding any auditing services provided.

27. Question: In Section IV.C.1, "telecommunications" is included in the list of "audits currently performed by University personnel or by the staff of contractors." We wanted to clarify whether JMU is looking for auditing support for telecommunications, or whether this telecommunications portion of the work falls more under the earlier description in the introductory paragraph of "various IT activities and processes" JMU needs (e.g., services more along the lines of voiceover IP, setting up virtual meetings). Any clarification of the type of work JMU requires in telecommunications that you could provide would be very helpful.

Answer: Audit of telecommunications only.

28. Question: Our company is fully qualified as a SWaM company and we have submitted our application for SwaM certification to the VA SBDB. However, we are unsure if we will have the certification at the time of proposal submission as we are expecting our certification sometime between now and December (depending on the turn-around time). Additionally, our firm is fully qualified to fulfill all aspects of the SON in the RFP. If our company does not receive the SWaM certification by the proposal submission date, but can show it is a candidate still awaiting certification, will it affect our proposal?

    Answer: SWaM status is evaluated during the RFP process but it is not a requirement for proposal submission. However, if applicable, vendors are strongly encouraged to apply for SWaM status.

29. Question: For proposal submission, is delivery of hard copy required, i.e. mail or hand delivery? Can proposals be emailed?

    Answer: JMU cannot accept emailed proposals. One (1) original and four (4) copies of the entire proposal, INCLUDING ALL ATTACHMENTS are required to be submitted in hard copy format. One copy shall also be submitted electronically (flash drive or CD). Any proprietary information should be clearly marked in accordance with 3.f.

30. Question: Does JMU require resumes of personnel proposed for support?

    Answer: Only for the primary person or persons

31. Question: Page 2 of the RFP states, "*Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP)." Are all personnel required to have the certs listed on above or is this simply providing guidance that the University required highly qualified and appropriately certified professionals?

    Answer: JMU would expect the primary person or persons who would be performing the work to have one or more of these credentials or similar qualifications.

32. Question: What is the size of the system(s) that fall under JMU's Audit and Management Services (AMS) (e.g., number of devices, number of hosts, number of databases, and number of wireless access points)?

    Answer: JMU's AMS is responsible for executing a risk-based audit plan, including IT infrastructure, systems and applications.

33. Question: How many applications does JMU AMS cover?

Answer: JMU's AMS is responsible for executing a risk-based audit plan, including IT infrastructure, systems and applications.

Signify receipt of this addendum by initialing *"Addendum #1_____"* on the signature page of your proposal.

Sincerely,
Doug Chester
Buyer Senior
Phone: (540-568-4272)