



**COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT**

Contract No. UCPJMU6764

This contract entered into this 11th day of December, 2023, 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 12/11/2023 through 12/10/2024 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 RFP FDC-1175 dated June 15, 2023
 - (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 No. One, dated July, 25, 2023
 - (e) Addendum No. Two, dated August 3, 2023
- (3) The Contractor's Proposal dated August 14, 2023 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
 - (a) Negotiations Summary, dated December 1, 2023
 - (b) Commonwealth of Virginia Agency Contract Form Addendum to Contractor's Form, dated October 31, 2023, which shall govern in the event of conflict.

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

CONTRACTOR:

By:  _____
(Signature)
karen cole
(Printed Name)
Title: Chief Executive Officer

PURCHASING AGENCY:

By:  _____
(Signature)
Doug Chester
(Printed Name)
Title: Buyer Senior

**RFP # FDC-1175 Information Technology Consulting Services
Negotiation Summary for Assura, Inc.**

December 1, 2023

1. Parties agree that this Negotiation Summary modifies RFP# FDC-1175 and the Contractor's initial response to RFP# FDC-1175, and in the event of conflict this negotiation summary shall take precedence.
2. Contractor's pricing schedule for the Purchasing Agency is as follows:
(All prices are in US Dollars and per hour rates)

Security and Federation Services	Onsite	Offsite
Principal Analyst/Consultant	324.90	270.75
Director	351.98	293.31
Engineer	241.30	280.25
Senior Engineer	370.50	308.75
Vice-President	379.05	308.75
C-Level Executive	433.20	361.00

Other Technology	Onsite	Offsite
Analyst I	182.40	152.00
Analyst II	208.05	173.38
Analyst III	239.69	199.74
Analyst IV	285.00	237.50
Analyst V	300.68	250.56
Analyst VI	304.95	254.13
Project Manager	169.29	141.08
Project Manager Senior	208.05	173.38

3. Onsite pricing shall be inclusive of all travel costs.
4. Billable hours shall be for actual work hours on authorized projects/tasks rounded to the quarter hour. Billable hours shall not include travel time.
5. Contractor shall provide detailed invoicing to include project title, number of hours worked onsite and/or offsite, role of individual(s) performing the work, and specific tasks performed.
6. 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.
7. The University may also request that these services be provided as a subscription service, as would be mutually agreed to prior to services being rendered, with deliverables determined by scheduled service requirements.
8. The Purchasing Agency reserves the right to reject any assigned personnel at any time with or without cause. Contractor shall provide a suitable replacement within a timely manner.
9. Contractor has disclosed all potential fees. Additional charges will not be accepted.

**COMMONWEALTH OF VIRGINIA AGENCY
CONTRACT FORM ADDENDUM TO CONTRACTOR'S FORM**

AGENCY NAME: James Madison University

CONTRACTOR NAME: Assura, Inc.

DATE: 10/31/2023

The Commonwealth and the Contractor are this day entering into a contract and, for their mutual convenience, the parties are using the standard form agreement provided by the Contractor. This addendum, duly executed by the parties, is attached to and hereby made a part of the contract. In the event that the Contractor enters into terms of use agreements or other agreements of understanding with University employees and students (whether electronic, click-through, verbal, or in writing), the terms and conditions of this Agreement shall prevail.

The Contractor represents and warrants that it is a(n) // individual proprietorship // association // partnership // corporation // governmental agency or authority authorized to do in Virginia the business provided for in this contract. (Check the appropriate box.)

Notwithstanding anything in the Contractor's form to which this Addendum is attached, the payments to be made by the Commonwealth for all goods, services and other deliverables under this contract shall not exceed Purchase Order Amounts; payments will be made only upon receipt of a proper invoice, detailing the goods/services provided and submitted to James Madison University. The total cumulative liability of the Commonwealth, its officers, employees and agents in connection with this contract or in connection with any goods, services, actions or omissions relating to the contract, shall not under any circumstance exceed payment of the above maximum purchase price plus liability for an additional amount equal to such maximum purchase price. In its performance under this contract, the Contractor acts and will act as an independent contractor, and not as an agent or employee of the Commonwealth.

The Contractor's form contract is, with the exceptions noted herein, acceptable to the Commonwealth. Nonetheless, because certain standard clauses that may appear in the Contractor's form agreement cannot be accepted by the Commonwealth, and in consideration of the convenience of using that form, and this form, without the necessity of specifically negotiating a separate contract document, the parties hereto specifically agree that, notwithstanding any provisions appearing in the attached Contractor's form contract, none of the following paragraphs 1 through 18 shall have any effect or be enforceable against the Commonwealth:


1. Requiring the Commonwealth to maintain any type of insurance either for the Commonwealth's benefit or for the contractor's benefit;
2. Renewing or extending the agreement beyond the initial term or automatically continuing the contract period from term to term;
3. Requiring or stating that the terms of the attached Contractor's form agreement shall prevail over the terms of this addendum in the event of conflict;
4. Requiring the Commonwealth to defend, indemnify or to hold harmless the Contractor for any act or omission;
5. Imposing interest charges contrary to that specified by the Code of Virginia, §2.2-4347 through 2.2-4354, Prompt Payment;
6. Requiring the application of the law of any state other than Virginia in interpreting or enforcing the contract or requiring or permitting that any dispute under the contract be resolved in the courts of any state other than Virginia;
7. Requiring any total or partial compensation or payment for lost profit or liquidated damages by the Commonwealth if the contract is terminated before its ordinary period;
8. Requiring that the contract be "accepted" or endorsed by the home office or by any other officer subsequent to execution by an official of the Commonwealth before the contract is considered in effect;

9. Delaying the acceptance of this contract or its effective date beyond the date of execution;
10. Limiting or adding to the time period within which claims can be made or actions can be brought;
11. Limiting the liability of the Contractor for property damage or personal injury. The parties agree that this clause does not extend the Contractor's liability beyond its own acts or those of its agents/employees;
12. Permitting unilateral modification of this contract by the Contractor;
13. Binding the Commonwealth to any arbitration or to the decision of any arbitration board, commission, panel or other entity;
14. Obligating the Commonwealth to pay costs of collection or attorney's fees;
15. Granting the Contractor a security interest in property of the Commonwealth;
16. Bestowing any right or incurring any obligation that is beyond the duly granted authority of the undersigned agency representative to bestow or incur on behalf of the Commonwealth.
17. Requiring the "confidentiality" of the agreement, in whole or part, without (i) invoking the protection of Section 2.2-4342F of the Code of Virginia in writing prior to signing the agreement (ii) identifying the data or other materials to be protected, and (iii) stating the reasons why protection is necessary.
18. Requiring the Commonwealth to reimburse for travel and living expenses in excess of the agency policy located at <https://www.jmu.edu/financemanual/procedures/4215mie.shtml>

This contract may be renewed annually by the Commonwealth after the expiration of the initial term under the terms and conditions of the original contract except as noted herein. If the Commonwealth elects to exercise the option to renew the contract for an additional renewal period, the contract price(s) for the succeeding renewal period shall not exceed the contract price(s) of the previous contract term increased/decreased by no more than the percentage increase/decrease of the "Other Services" category of the CPI-W of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

This contract has been reviewed by staff of the agency. Its substantive terms are appropriate to the needs of the agency and sufficient funds have been allocated for its performance by the agency. This contract is subject to appropriations by the Virginia General Assembly.

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

AGENCY by 
Title Buyer Senior
Printed Name Doug Chester

CONTRACTOR by 
52AE0F655128412...
Title Chief Executive Officer
Printed Name Karen Cole

October 2022

James Madison University

Information Technology Consulting Services

RFP# FDC- 1175

Proposal Submitted to

Doug Chester
Buyer Senior
Procurement Services



Submitted by



7330 Staples Mill Rd.
#292
Richmond, VA 23228 USA
<https://assurainc.com>
SWaM Number 661749
SCC Entity ID : 06752125

Contact: Karen Cole, CISA, CRISC,
CBCP, MBCI
Email: karen.cole@assurainc.com
Phone: (804) 767-4521

Date: August 15, 2023

7330 Staples Mill Road
#292
Richmond, Virginia 23228
Web: www.assurainc.com
Phone: 804-672-8714



August 15, 2023

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

Re: Request for Proposal# FDC-1175: Information Technology Consulting Services

Dear Mr. Chester:

Assura sincerely thanks James Madison University (JMU) and the Virginia Association of State College and University Purchasing Professionals (VASCUPP) respectively for the opportunity to respond to RFP # FDC-1175 titled *Information Technology Consulting Services*. Assura has enjoyed successfully working with JMU, VASCUPP member organizations, and authorized users of this contract over the past 5 years to deliver our services. We are genuinely excited about the potential opportunity to continue to work with your organizations.

As our proposal demonstrates, Assura is a full-service Virginia-based cybersecurity firm that is ready to meet JMU's needs now and in the future. We not only have significant experience working within the education industry, but with various government organizations that continue to rely on this contract for procurement of critical cybersecurity and information technology services. Our extensive experience, industry leading consultants, excellent tools, and proven methodologies not only meet but exceed our clients' expectations. Assura brings the management, operational, technological, regulatory, and information security expertise necessary to deliver any project successfully, on time, and on budget.

At Assura, we are invested in the success of your organization. We work hard to be your trusted advisor, provide extra helping hands when needed, and be your security and information technology champion. We commit to take away the pain of technology and cybersecurity while we help you enjoy the experience of seeing your operations grow and flourish. Through our AuditArmor™ Guarantee, we commit to delivering products and services that are fully compliant with all applicable regulations while meeting the organization's information technology and security goals.

We have made every attempt to provide detailed information regarding our service offerings and associated costs based upon the RFP. However, we understand that there may be additional considerations regarding the purchase of our tools and services. Therefore, we are happy to have follow up discussions needed to ensure that JMU and other VASCUPP members take advantage of all services and potential discounts.

Request for Proposal RFP# FDC-1175

We remain at the ready to help you reach your information technology and security goals. If you or your team have any questions about our proposal or capabilities, please do not hesitate to contact me via telephone at (804) 767-4521 or email at karen.cole@assurainc.com.

Sincerely,



Karen L. Cole, CBCP, CISA, CRISC, MBCI, CMMC RP
CEO

James Madison University

Information Technology Consulting Services

RFP # FDC-1175

REDACTED

Proposal Submitted to

Doug Chester, VCO, CUPO
Senior Buyer
James Madison University



Submitted by










7330 Staples Mill Rd.
#292
Richmond, VA 23228 USA
<https://assurainc.com>
SWaM Number 661749
SCC Entity ID : 06752125

Contact: Karen Cole, CISA, CRISC, CBCP,
MBCI, CMMC RP
Email: karen.cole@assurainc.com
Phone: (804) 767-4521

Date: August 15, 2023

TABLE OF CONTENTS

1.0 RFP Cover Sheet and Addenda Acknowledgements	3
2.0 Statement of Needs Response	4
2.1 Competencies and Experience	7
2.2 Methodologies	10
 2.2.1 Fractional Information Security Officer Services (Virtual ISO)	11
 2.2.2 Managed Security Services Including SIEM	13
 2.2.3 Penetration Testing	22
 2.2.4 Vulnerability Management-as-a-Service (VMaaS)	29
 2.2.5 Multifactor Authentication (MFA)	31
 2.2.6 ProDefense	32
 2.2.7 Advisory Services	35
2.2.8 Security Life Cycle for Amazon Web Services	36
2.3 Personnel	37
2.4 Consultants Continuity Plan	41
2.5 Available Services	41
2.6 Training and Documentation	42
2.7 Recent Projects	44
2.8 Knowledge Transfer	46
2.9 Project Management	47
2.10 Functional Staffing	48
2.11 Subcontracting Plan	48
3.0 Attachment A: Offeror Data Sheet	49
4.0 Attachment B: Small Business Contracting Plan	50

5.0 Sales with VASCUPP Member Organizations	52
6.0 Proposed Pricing Schedule	54
Reference: Original RFP	57
Reference: Addendum 1	85
Reference: Addendum 2	92

1.0 RFP Cover Sheet and Addenda Acknowledgements

REDACTED

2.0 Statement of Needs Response

James Madison University (JMU) is a dynamic organization helping students to achieve their dreams with its unique approach to delivering education through engaged learning. JMU sets itself apart from other universities by being a community committed to preparing students to be educated and enlightened citizens who lead productive and meaningful lives.

One of the backbones to delivering on its mission to students and stakeholders, is ensuring the prudent management of information technology to prepare them for the global, digital, and information economy. While technology is a core enabler of growth in our society, there is also a significant responsibility for ensuring that technical capabilities are delivered in a manner that protects the organization and the user. This responsibility is fulfilled by a combination of program management actions and the utilization of robust tools.

Assura understands that JMU, and other Virginia Association of State College and University Purchasing Professionals (VASCUPP) organizations, must deliver technology in a manner that is dynamic, robust, and responsive to the needs of the organization all the while maintaining safety and security for everyone.

We work with our clients to achieve their organizational goals while being sensitive to constraints such as time, resource bandwidth, and budget.

About Assura

Assura is the premier cybersecurity and information technology organization for JMU and VASCUPP member organizations because they require seasoned consultants that are invested in not just the success of the technology and supporting security, but also the success of the organization. Assura is proud of its 95% client retention rate. Our clients select us when they want:

- ✓ Dynamic information security programs, support services, and industry leading tools from OEM partners such as Amazon Web Services (AWS), Microsoft, AT&T Cybersecurity, Huntress, SentinelOne, Duo, and KnowBe4.
- ✓ Expert support delivered by seasoned practitioners that can quickly identify and solve even the most complex problems and provide an extra set of helping hands when needed with fractional information security officer services such as Virtual ISO;
- ✓ Taking the pain of technology implementation, management, security, and update away and ensuring your program achieves and maintains compliance with multiple regulatory and industry standards; and
- ✓ Doing all of this while supporting your regular information technology and security functions as needed and keeping you safe and operational.

Assura, Inc. ("Assura") is a Richmond, Virginia based small-woman-owned consulting firm created in 2007 that is focused on information technology and cybersecurity services across all practice and operational areas. Our managed Governance, Risk and Compliance (GRC) services coupled with our managed information technology services provide full coverage to meet any JMU and VASCUPP member's technology needs. Our company is proud to be a certified as a:

Assura is the right choice!



Information Security is Who We Are

At Assura, we are safeguarding the future one client at a time. Our experts lead the industry in taking the pain of information security away from our clients. Let us give you back your piece of mind!

No Risk with Our Audit Armor™ Guarantee

Selecting your information security partner should be the safest thing you ever do. Our unique guarantee makes using us even safer! It simply means that we are so confident in our work that if any of our materials are out of compliance, we will fix them for free. If our materials are audited, we will defend them for free. It's that simple. You only get this with Assura!

Experts Securing Your Future

We are experts in information security across many different regulations and frameworks such as HIPAA, NIS1, PCI DSS, FFIEC – to name a few. We not only bring the program planning, but also the staffing and tools to meet all of your program needs. We are the right choice when you want not just compliance, but program excellence!

Creative Problem Solvers

No two clients are a like – neither are their IT management and security needs. Our developed tools are a springboard to getting quick results while we customize your program. Our working consultants do the work so that your leaders can lead!

- Small Woman and Minority Owned (SWaM) certified Small, Woman-Owned business by the Virginia Department of Small Business and Supplier Diversity (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 listed on the Inc. 5000 list of fastest growing companies in the United States for the past **three** years. In 2023, Assura was listed as one of the 24 Virginia companies on the Inc. Best Workplaces in the U.S. list. In 2016, Assura was 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.

Requirements and Experience

The purpose of the following sections of this proposal is to provide JMU and VASCUPP members with an overview of the extensive information technology and cybersecurity capabilities of our firm.

At Assura, we are experts in marrying the compliance requirements of standards such as National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI), International Organization for Standardization (ISO). With respect to cybersecurity, we have extensive experience with the Cybersecurity Framework (CSF), NIST 800-171, Special Publication 800-53 (currently used by several colleges, universities, and government organizations), ISO 27001, Payment Card Industry Data Security Standard (PCI DSS), FERPA, and HIPAA with the business needs and security objectives of organizations.



While compliance is not the sole driver for performing information technology and security activities, it is important for heavily regulated organizations such as public colleges and universities. In addition to providing services that are compliant across multiple standards, we also provide our Audit Armor Guarantee. **No one else in the industry does this.**

Our guarantee is simple. If you are audited, Assura has you covered. Our AuditArmor® Audit Defense Guarantee means that we guarantee our work to be compliant with the identified cybersecurity frameworks and regulatory requirements (unless waived by you). We defend our work at no additional cost. Yes, we're serious. And yes, we're that confident in the quality of our work. We have you covered from audit entrance conference to exit conference and will work with your auditor or regulator to defend our work. On the off chance that a change needs to be made to the deliverable, we'll do that for free. It's that simple.

Assura is pleased to provide a response to the statement of needs as identified in the RFP. To ensure that the information provided is responsive to the requirements of the RFP and easy to reference, we have broken up the following information across Section 2.

Section	Section Title	RFP IV Mapping and Description	Proposal Page Number
2.1	Competencies and Experience	<ul style="list-style-type: none"> • Maps to IV.1 • Services Overview 	7
2.2	Methodologies	<ul style="list-style-type: none"> • Maps to IV.2 • Detailed Methodologies • Tools Overview • Management for Scope of Projects 	10

Section	Section Title	RFP IV Mapping and Description	Proposal Page Number
2.3	Personnel	<ul style="list-style-type: none"> • Maps to IV.3 • Names, Qualifications, and Experience of Personnel • Primary Contact 	37
2.4	Consultants Continuity Plan	<ul style="list-style-type: none"> • Maps to IV.4 • Consultants Continuity Plan 	41
2.5	Available Services	<ul style="list-style-type: none"> • Maps to IV.5 • Additional Services Not Detailed in section 2.1 or 2.2. 	41
2.6	Training and Documentation	<ul style="list-style-type: none"> • Maps to IV.6 • Training Methodology and Tools 	42
2.7	Recent Projects	<ul style="list-style-type: none"> • Maps to IV.7 • Recent Projects Overview 	44
2.8	Knowledge Transfer	<ul style="list-style-type: none"> • Maps to IV.8 • Knowledge Transfer 	46
2.9	Project Management	<ul style="list-style-type: none"> • Maps to IV.9 • Project Management 	47
2.10	Functional Staffing	<ul style="list-style-type: none"> • Maps to IV.10 • Functional Staffing 	48
2.11	Subcontracting Plan	<ul style="list-style-type: none"> • Maps to IV.11 • Subcontracting Plan 	48

For additional detail, please refer to the Table of Contents for this proposal.

2.1 Competencies and Experience

RFP Requirement: “IV.1. Provide detailed corporate competencies/experience serving one or more of the technologies listed below.”

Assura is responding the following technology areas:

- c. Desktop and Mobile Device Management
- d. Microsoft Azure and M365
- e. Security and Federation Services; and
- l. Other Technology.

The purpose of this section is to provide JMU and VASCUPP members with an overview of Assura’s extensive information technology and cybersecurity capabilities of our firm. This section also provides a reference to Section 2.2 Methodologies which goes into greater detail regarding the approach and methodologies for each service.

Services Overview

This section details the high-level services contained within this proposal. There are a number of services that map to the requested RFP services: IV.1.c. Desktop and Mobile Device Management, IV.1.d. Microsoft Azure and M365, IV.1.e Security and Federation Services, and IV.1.l Other Technology. The table below details Assura’s proposed service, a high-level description of the service, and the RFP requested service to which it maps.

Service	Description	Maps to Statement of Need
Advisory Services	Project based information security and information technology services. Customized client services across all areas to address new, emerging, and lingering technology needs.	c. Desktop and Mobile Device Management d. Microsoft Azure and M365 e. Security and Federation Services l. Other Technology
Amazon Web Services	Amazon Web Services (AWS) provides a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications.	l. Other Technology
Fractional Information Security Officer Services (Virtual ISO)	Fractional Chief Information Security Officer Services for organizations that do not have the need or budget for a full-time officer.	e. Security and Federation Services
Managed Security Services Including SIEM	Managed cybersecurity services that are integrated to ensure that all services are performing in alignment with client requirements and expectations.	e. Security and Federation Services

Service	Description	Maps to Statement of Need
Multifactor Authentication (MFA)	Managed MFA services to reduce the risk of account takeovers and provide additional security for users and their accounts.	e. Security and Federation Services
Penetration Testing	Targeted and safe testing as a simulated cyber-attack against client systems to determine exploitable vulnerabilities.	e. Security and Federation Services
ProDefense	Deployment of end-user information technology and cybersecurity solutions in a fully compliant environment that is a full lifecycle solution. Users can be onsite or remote.	c. Desktop and Mobile Device Management d. Microsoft Azure and M365
Vulnerability Management-as-a-Service (VMaaS)	Ongoing managed service for system vulnerability identification, reporting, remediation, and management.	e. Security and Federation Services

Please use the following legend when referencing standards acronyms from this proposal:

Acronym	Definition
ANSI	American National Standards Institute
COBITv5	Control Objectives for Information and Related Technologies Version 5
FERPA	Family Educational Rights and Privacy Act
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act of 2002
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
ISO/IEC 27001	ISO/IEC 27001:2013 Information technology – Security Techniques – Information security management systems – Requirements
ISO/IEC 27002	ISO/IEC 27002:2013 –Security Techniques – Code of Practice for Information Security Controls

Acronym	Definition
NIST	National Institute of Standards and Technology
NIST 800-53	NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
NIST CSF	NIST Cybersecurity Framework
PCI DSS	Payment Card Industry Data Security Standards

2.2 Methodologies

RFP Requirement: “IV2. Describe approach and methodology to providing IT consulting services to James Madison University. Include how your firm would manage the scope of projects.”

Assura consultants are experts covering all areas of information security, information technology, and compliance. Since 2007, our company has perfected the services detailed in this section by ensuring that our products not only address new and emerging threats, but also stand the test of time. With a mixture of best practices, compliance requirements, and our own hands-on experience, we have crafted our approach and methodologies to ensure success for our clients during each engagement.

The methodologies listed here are just the beginning. Our clients have unique needs, and we customize each methodology to meet their unique requirements. We are not just turning out the same solutions over and over. We are taking the pain of security and compliance away for our clients.

The following methodologies are organized as follows:

Section	Service	Maps to Statement of Need
2.2.1	Fractional Information Security Officer Services (Virtual ISO)	e. Security and Federation Services
2.2.2	Managed Security Services Including SIEM	e. Security and Federation Services
2.2.3	Penetration Testing Services	e. Security and Federation Services
2.2.4	Vulnerability Management-as-a-Service	e. Security and Federation Services
2.2.5	Multifactor Authentication (MFA)	e. Security and Federation Services
2.2.6	ProDefense	c. Desktop and Mobile Device Management d. Microsoft Azure and M365 e. Security and Federation Services
2.2.7	Advisory Services	e. Security and Federation Services I. Other Technology
2.2.8	Amazon Web Services	I. Other Technology



2.2.1 Fractional Information Security Officer Services (Virtual ISO)

Successful implementation of any information technology or cybersecurity program starts at the very top of the organization. Assura's Virtual Information Security Officers (Virtual ISOs) are trained to understand the needs of all levels of program participants in the organization from the Board and executive leaders to the individual frontline worker.

Our consultants know how to translate complex and technical policy and program requirements in a language that is understood by leadership; as well as having detailed technical discussions with IT leadership and support staff in a manner that they understand.

One of the most important areas where these skills are critical is in the development of policies, procedures, and plans for various information technology and information security standards. Assura not only partners with its clients to educate them on the control requirements, but to also provide options so that they may make informed business decisions that are codified in the policies and procedures. After our consultants develop these items, they facilitate the process to obtain approval from the highest levels of the organization.

Upon completion of the policies and procedures, Assura will work with the client to develop all of the program artifacts to implement the necessary controls. From analysis to plan development, Assura has you covered.

Please see the next page for many of the different types of deliverables provided by our Virtual ISO service.

The age of Democratizing Cybersecurity® is here.

At Assura we believe cybersecurity isn't a privilege, it's a right.

That's why we offer scalable solutions that fit the budget for any organization and will work hard to make sure you have the protection you need. We deliver world-class cybersecurity to organizations guaranteed to meet or exceed compliance regulations.

How does Virtual ISO™ solve your security and compliance challenges?

- We map out a fully functional and compliant program, then build it together
- You're guided through all program management decisions
- You decide how your organization will run the business end of cybersecurity
- All the unsexy work of documentation will be taken care of by your Virtual ISO™ team
- Your IT experts implement the necessary technical safeguards
- We work closely with your IT folks to make sure your system is secure
- Once the program is in place we continue to keep it maintained and compliant going forward
- Users are trained in security practices to help defend against attacks
- We take on cybersecurity planning activities such as system security plans if applicable
- In the unfortunate event of a cyber incident, we advise on how to handle it

What do you get with Virtual ISO™?

- Fractional Chief Information Security Officer (CISO)
- Security policies, standards, and guidelines
- Security processes, procedures, and plans
- Business Impact Analysis
- Security awareness training
- Security and compliance assessments
- Risk assessments
- Third-party vendor oversight
- Secure system development
- Investigate and lead response to security breaches
- Recurring compliance activities management
- Audit defense with AuditArmor™



2.2.2 Managed Security Services Including SIEM

Assura is proposing its Managed Security Incident and Event Management (SIEM) services. The Managed SIEM service comes with the following features and benefits:

- Primary and secondary Concierge threat analysts
- Cloud-based dedicated portal with reporting dashboards and real-time analytics
- 24/7/365 data collection and response
- AI-based event correlation, threat hunting, and alerting
- Human analysis of all alerts
- Active human-based threat hunting
- Root cause analysis of security incidents
- 1-hour notification SLA of confirmed or suspected security incidents
- 1-hour SOC response-time SLA guaranteed any time day or night
- Network Intrusion Detection System
- Real-time threat intelligence integration
- Custom reporting
- 90-days of online searchable event storage
- 365-days of cold storage of all events
- Monthly web meeting reporting conferences with expert trend analysis, recommendations for security and compliance posture strengthening, and service check-ins
- AuditArmor™ Compliance Guarantee
- AuditArmor™ Audit Response Support

Assura's US-based Virtual SOC (vSOC) is in Richmond, VA. We maintain service continuity through our use of a cloud-based platform, AT&T Cybersecurity's AlienVault Unified Security Management Anywhere (USMA) which provides us with the ability for all vSOC personnel to support our clients from Virginia as well as (at the time of this proposal) three other states.

Our vSOC operates 24 hours per day, 7 days per week, 365 days per year and supports dozens of clients throughout Virginia, including independent Virginia state commissions, colleges, and universities as well as state agencies and localities. Our vSOC is staffed by exclusively by Assura employees and we do not subcontract or outsource our vSOC to any other party.

Our vSOC personnel have a combination of CISSP, CISM, GCED, CEH, Security+, eCPPTv2, and other certifications. The director of our vSOC has 13 years of computer systems defense, threat intelligence, and threat hunting capabilities. Our Chief Technology Officer has 26 years of experience in computer systems defense, threat tactics, and cyber risk governance. Our SOC analyst team has an average of 7+ years of experience with computer systems defense and threat hunting capabilities.

vSOC analysts are expected to maintain their knowledge, skills, and abilities by:

1. Maintaining one or more cybersecurity certifications. Assura pays for educational courses that count as Continuing Professional Education (CPE) credits.
2. Learning the latest Tactics, Techniques, and Procedures (TTPs) used by threat actors by reviewing threat intelligence analyses from Information Sharing and Analysis Centers, US-CERT, and the Cyber and Infrastructure Security Agency (CISA) component of the US Department of Homeland Security (DHS).
3. Maintain practical, hands-on experience of TTPs through regular challenges through the Hack The Box and LetsDefend platforms.
4. Briefings on attack techniques from our both our penetration testing and Digital Forensics and Incident Response (IR) teams.
5. Participating in retrospectives of real security incident investigations for clients.
6. Participation in "purple team" exercises where our penetration testing team tests the detection capabilities of our vSOC team.

All Assura personnel must be legal residents of the United States of America and must be eligible for employment in the United States without the company sponsoring a work visa. All staff are background checked for criminal history in all 50 states and the District of Columbia, sex offender registries, driving record, SSN trace, address, DOB, and name verification. For certain positions, we also conduct an education verification.

All of our Software-as-a-Service (SaaS) platform partners where the organization's data would be stored have a SOC-2 Type 2 report. In order to fulfill the assessment requirements RFP, we are happy to facilitate the client receiving copies of these reports.

Much of our internal infrastructure is built in Amazon Web Services and Microsoft Azure. Evidence of their SOC 2 Type II reports as well as many other cybersecurity certifications can be found at:

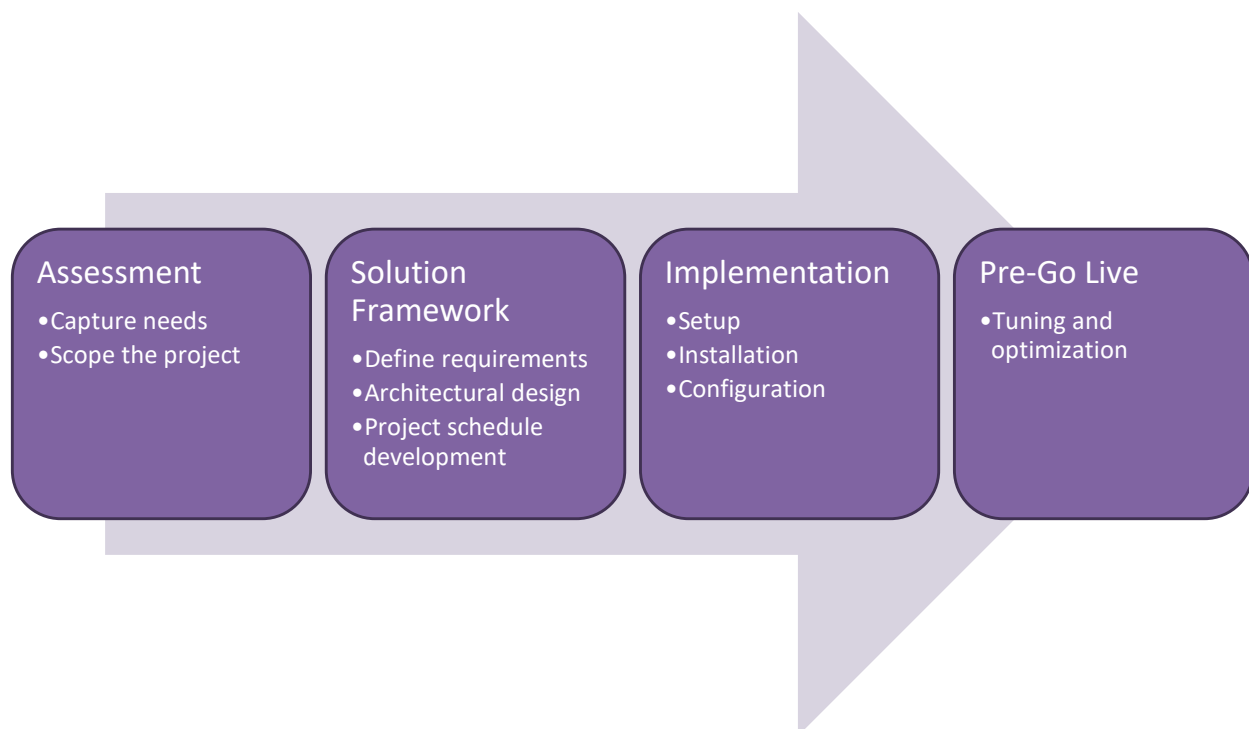
Amazon Web Services: <https://aws.amazon.com/compliance/programs/>

Microsoft: <https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide>

Deployment Methodology

Assura employs a two-phase methodology to deliver its Managed SIEM service. This can be done independently or in conjunction with other service offerings from Assura and is often the logical next step for many clients after receiving a security assessment from Assura as it provides an end-to-end ongoing service that can fill gaps in their security program. As an adaptive security service, it is both scalable and flexible enough to meet the needs of a wide range of client environments from small single office clients to large global enterprise networks with tens of thousands of users. Assura will tailor a custom implementation plan for each client.

Phase I – Assessment and Provisioning



Assessment

Capture Needs – During the initial stages of the engagement, Assura works with a client to capture their needs defined within the five pillars itemized above. If not already understood by the client, an assessment of the environment can be provided to help define this. If a client has previously separately purchased one of these assessment solutions offered by Assura, it will be utilized to fulfill this need provided that the assessment is still current enough to accurately capture needs.

Scope the Project – A full scoping of the project will be conducted to ensure that all aspects of the clients' environment, where adaptive security is needed, are inventoried. Assura engineers will work closely with the IT staff to ensure that all systems relevant to the ASA are identified and cataloged.

Solution Framework

Define Requirements – Once the project is scoped, technical and procedural requirements can be crafted to help build the solution framework. Documentation will be provided including a plan for the implementation of the service.

Architectural Design – After requirements are defined a services solution architecture is designed to meet these requirements and serve as the primary guiding document for the implementation.

Project Schedule Development – Finally, once architected, an initial project schedule can be built to track tasks and the timeline for the client. A periodic review of the project schedule will be conducted with the client as needed or requested. In most environments, Assura can have the service installed and operational in a very short time frame but delays due to client business requirements may delay implementation.

Implementation

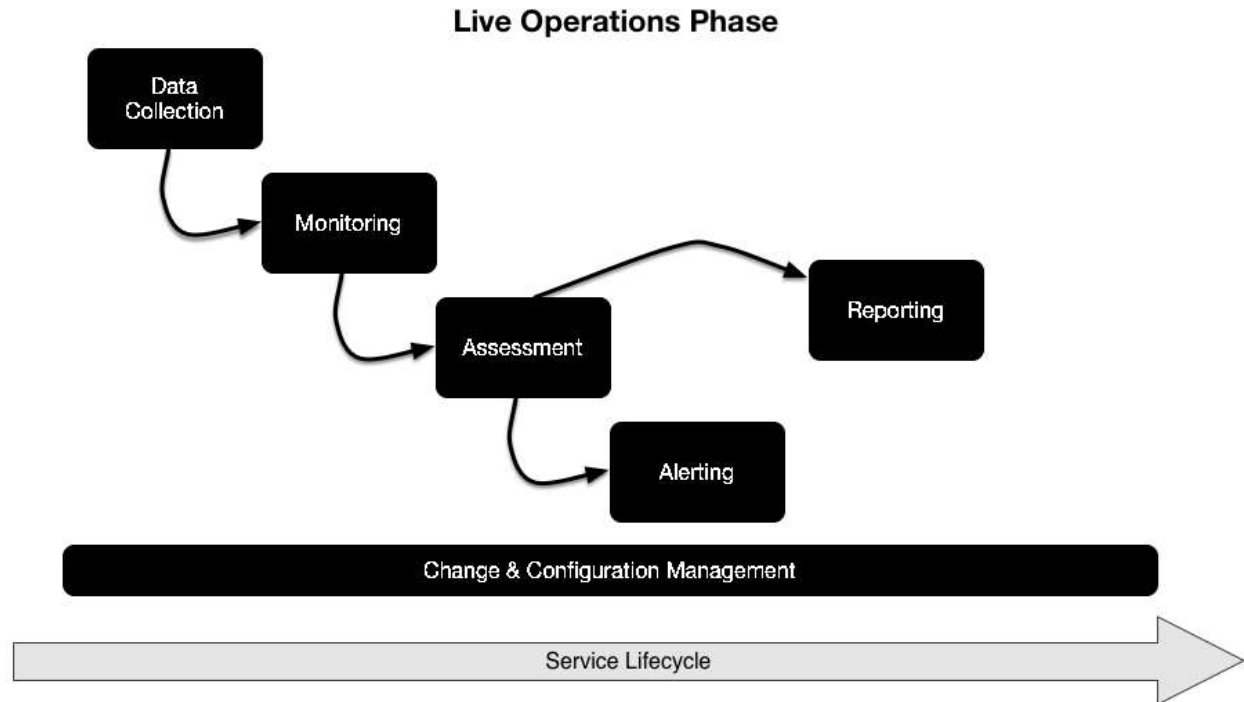
Setup – During this phase Assura works closely with the Client to prepare the enterprise environment to receive the necessary components of the service prior to installation. This will vary depending on how the service is architected for the environment but can include physical considerations such as: rack space, power & virtualization, as well as network considerations to allow connectivity of those components. The service components are designed to have a small footprint, but the size and distribution of a network along with the client requirements determine the placing of the sensors.

Installation – All necessary hardware & software is installed per the design requirements. Should the Client cancel the Managed SIEM Service, Client will be required to return any provided equipment including all shipping materials. Hardware for these components should be dedicated for the Managed SIEM and not shared with other applications. If Assura determines that Client's equipment can be used the client must maintain the underlying equipment to Assura's standards.

Configuration – The service components are configured and customized for the network environment. This can be done in an all-in-one session or in phases depending on the needs and schedule of the client.

Pre-Go Live

Tuning and Optimization – Any areas for tuning discovered during the acceptance testing will be addressed. While planning for an installation is exhaustive and thorough, there are occasions where unforeseen or unanticipated outcomes occur (e.g., policy, network or other changes that change the volume or nature of the logging data capture) where further tuning of the installation is required. Typically, these are minor in nature but are reviewed in the interest of being thorough. Although Assura strives to adequately engineer the solution, unanticipated situations such as devices set for excessive logging levels (e.g., debug) could result in engineering modifications that result in changes to pricing and implementation schedule.



Phase II – Live Operations

Go-Live – At Go-Live, the security service becomes operational, and Service Level Agreements go into effect. Through continuous data collection, the Assura SOC begins monitoring and assessing the client's enterprise and keeps the designated contact(s) alerted and informed of any relevant security events. Reports are delivered per scheduled commitments. Assura will also meet with the client at least annually or more frequently if needed to ensure the service is meeting their needs. Assura maintains a staff of engineers that are experts with the Assura Managed SIEM service and underlying technologies.

Service Delivery Scope Changes – As a network environment grows, so too can the service. When new hosts, network devices, domains, and other elements are introduced the Managed SIEM may be configured to cover these new requirements. These changes may require a contract update.

Configuration Changes – Often clients can have security policies change over the course of time. Those changes can affect the entire domain or be limited to a specific host or group of hosts. Flexibility and comprehensive coverage of the network are two high value features of the service. IT environments are by their nature, ever changing, growing and evolving. The Managed SIEM service is capable of keeping pace with the breadth and depth of all these changes to ensure the service is never compromised or dated. In the case of changes, to ensure the client's environment is supported appropriately, Assura may require a contractual update and/or Professional Services to meet these scope changes.

Solution Components

Assura's Managed SIEM solution is comprised of the following components:

1. The AlienVault USMA Software-as-a-Service platform. This component is where all log data is stored, correlations are run, threat intelligence feeds match indicators of compromise to the log data, the platform is configured and managed, and users log in to view and interact with dashboards, reports, and data.

The AlienVault USMA platform comes "out of the box" with hundreds of correlation rules for the most common types of attacks. However, Assura also applies a set of custom correlation and alerting rules based on its knowledge and experience. We also develop and apply custom correlation and alerting rules based on patterns of behavior we identify within the environment and discuss with the client. We have a live threat feed that updates known Indicators of Compromise (IOCs) in real time that provides the platform with visibility into new and emerging

threats nearly instantaneously. The AlienVault agent provides us with the ability to identify unauthorized tampering of operating system and service files/executables, and rootkit detection.

Assura also leverages a live threat intelligence feed from AT&T Cybersecurity -- Open Threat Exchange (OTX). OTX is a crowdsourced threat intelligence and reporting platform with over 19 million threat indicators rules contributed daily by over 100,000 global participants (including Assura). OTX is also how the AlienVault NIDS receives updated Emerging Threats rules curated by AT&T Cybersecurity's AlienVault Labs.

All data is transmitted to the USMA platform via Transport Layer Security version 1.2 with the ECDHE-RSA-AES-256-GCM-SHA384 cipher suite. All data at rest is protected with AES-256 encryption.

2. Sensors placed in the data centers. These sensors are virtual appliances compatible with Hyper-V and VMware. Each sensor runs a combination of open source and proprietary tools to collect event logs, perform network intrusion detection, and conduct vulnerability scanning. These include:
 - Suricata: Network Intrusion Detection (NIDS) that uses a Snort-like syntax to inspect traffic on the network. The Network Intrusion Detection System provided by our on-prem AlienVault USMA sensor provides real-time inspection of network traffic based on detection rules published by Emerging Threats, a division of Proofpoint. These rules are used by numerous intrusion detection and intrusion prevention products outside of USMA. For more information about Emerging Threats, please see https://doc.emergingthreats.net/bin/view/Main/EmergingFAQ#What_is_Emerging_Threats
 - Syslog-ng: Depending on the data source/asset type, data can be collected at the sensor via syslog (UDP 514), syslog TCP (TCP 601 or 602), and syslog TLS (TCP 6514 or 6515). Many data sources receive events via API integration (for example most SaaS applications and some on-premises devices such as firewalls). Ingestion of event information from some applications.

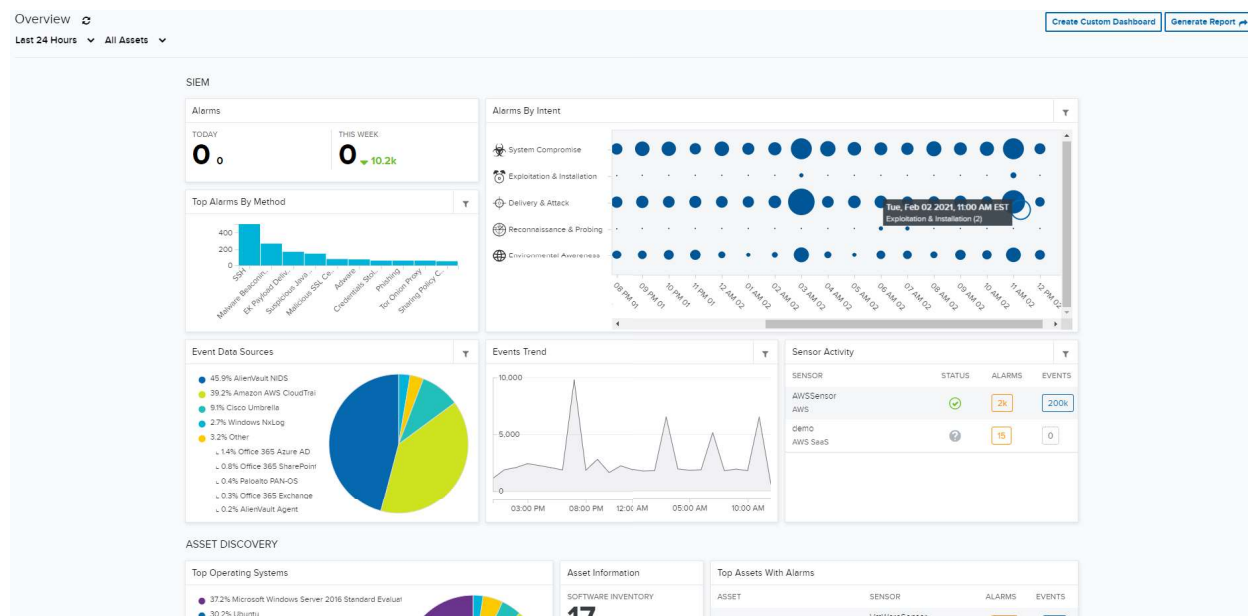
Each sensor requires 12 GB of dedicated RAM, 4 vCores, and 150 GB of storage. Each sensor needs to have one physical network port and at least one additional network port connected to a vSwitch dedicated to it. The dedicated port is used to receive network traffic for the NIDS function and the other is used for management and to receive logs from local devices such as firewalls and from systems loaded with the NxLog agent (see below for a description of the NxLog agent).

3. AlienVault Agent built on the osquery engine. Osquery is an open-source project with AT&T Cybersecurity as a major contributor. Its purpose is to transmit operating system logs from Windows systems to the AlienVault platform. Another function is to provide detection of malicious payloads, shellcode, and rootkits using YARA rules. It also provides file integrity monitoring within key operating system directories. Finally, the agent allows us a means of pulling forensic information from assets such as registry keys, running processes, established network connections, and other vital information. The AlienVault agent sends events directly to the USMA cloud platform, which means for continuity's sake, we can receive operating system logs irrespective of the status of the sensor.
4. While the AlienVault agent delivers operating system logs to our platform, another agent, NxLog, provides a means of collecting logs from services such as IIS, Apache, Microsoft DNS, Microsoft DHCP, Microsoft Exchange, and the plethora of others.
5. The Huntress agent is installed on all Windows servers. The purpose of the Huntress AI-based threat hunting agent is to actively search for persistent footholds and other indicators of threat activity. As part of its early warning system, the Huntress agent drops canary files on the systems on which it runs so that it can quickly detect and report the presence of ransomware to the Assura vSOC.

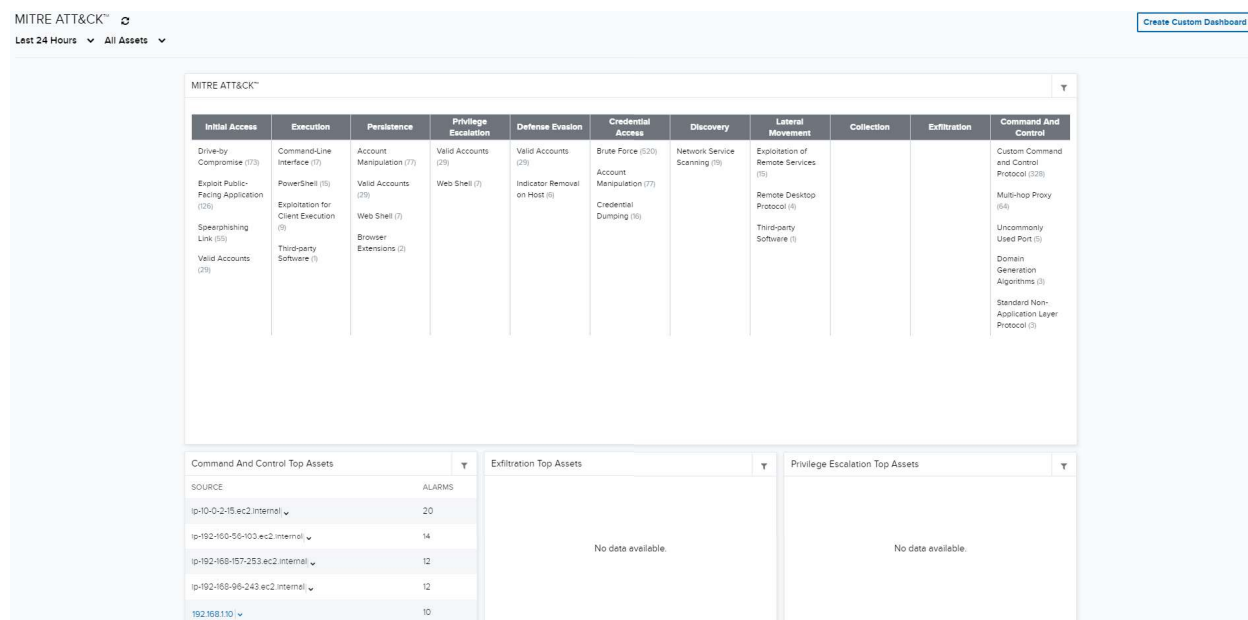
Authorized users will have access to the USMA portal to be able to access dashboards showing alarms, vulnerabilities, NIDS events, and numerous other topics of interest. Users can create custom dashboards

with drag-and-drop widgets to present the most important information to them in the way that they want. Users can then drill down into details of alarms, events, and vulnerabilities.

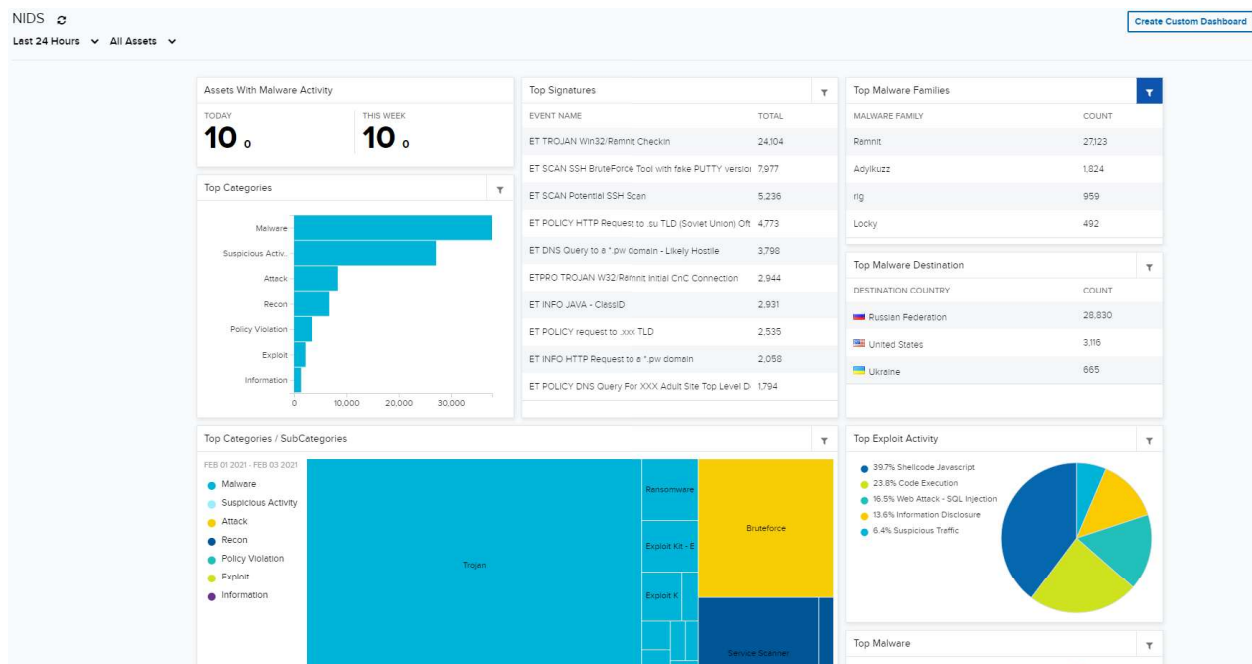
Below is a sample of an overview dashboard:



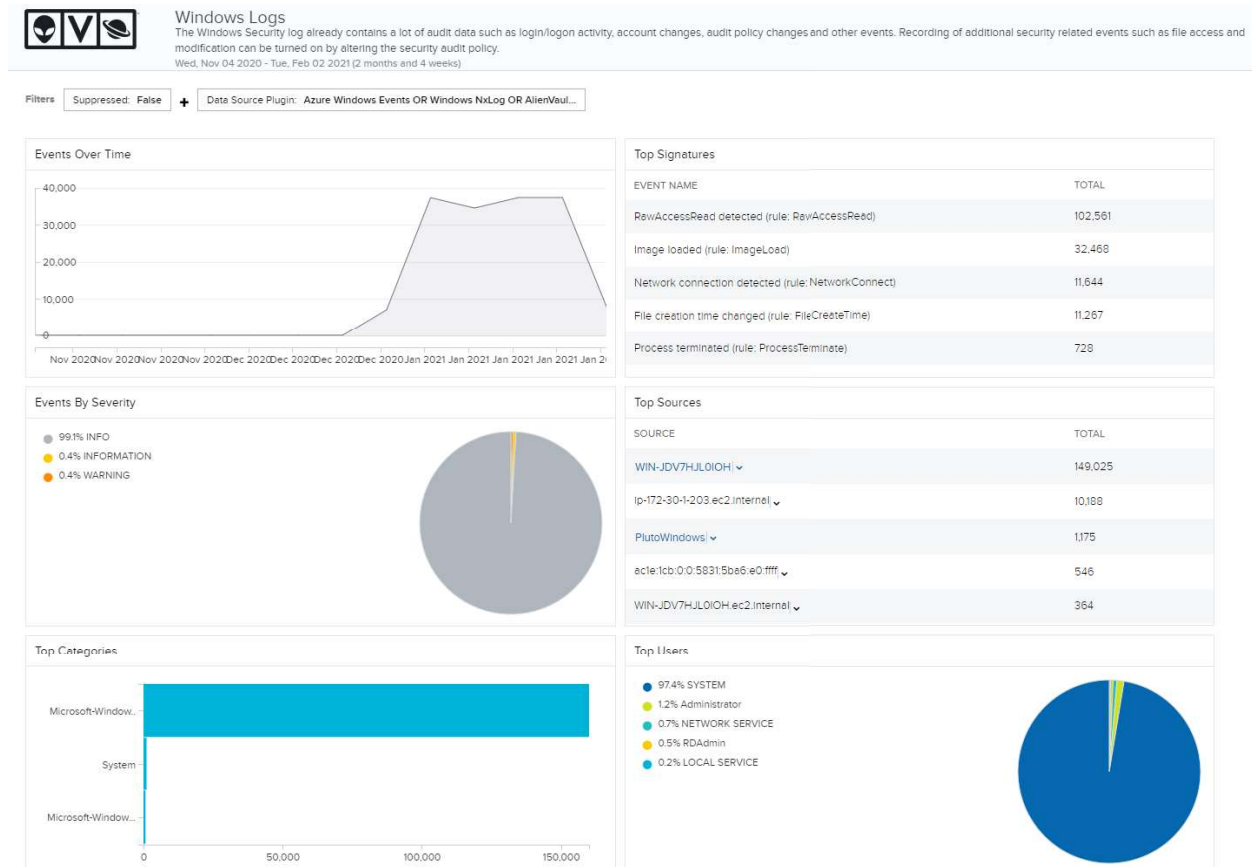
This dashboard presents attacks by elements within the MITRE ATT&CK framework:



This dashboard presents NIDS detections:



This is a custom report that presents Windows event information:



Investigations and Incidents

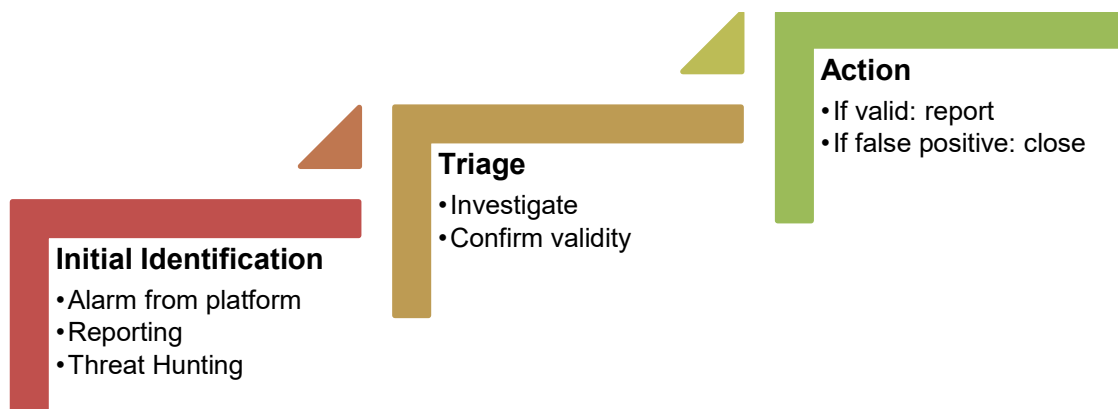
Our vSOC analyzes events in two primary ways:

- The correlation rules and IOC identification in our SIEM platform surface automated alarms to our SOC analysts where those alarms are investigated.
- Our vSOC analysts conduct threat hunting “play books” by reviewing trends within event logs in our SIEM platform that indicate suspicious activity.

Alarms are designated as Low, Medium, and High. Alarms are reported to the client as follows:

- **Low:** Reported weekly in a rollup report.
- **Medium:** Best effort reported within 24 hours.
- **High:** Treated as a Security Incident as defined below.

A “Security Incident” is defined as an activity or series of activities on a monitored asset that Assura’s vSOC deems to be a confirmed imminent threat to the confidentiality, integrity, and/or availability of customer data. Clients are notified of confirmed security incidents; suspicious events or patterns of behavior where only someone with access to an asset (or group of assets) can assist with confirmation of the validity of the incident; or when we see a disruption to the flow of information to the vSOC as illustrated in the diagram below.



Clients are notified via email ticket, text message, and/or telephone call depending on the severity of the incident. Each client designates a call list with prioritized contacts, contact information, and preferred contact method. This is all customizable and matches the client’s priorities and workflows.

In a case where there is a confirmed breach, clients have the option of engaging Assura’s Digital Forensics and Incident Response (DFIR) team or working with their cyber insurance carrier. In some cases, our clients request appointment of Assura as their panel forensic provider. This is why we are appointed as one of the panel forensic providers for a statewide insurance risk pool.

Our DFIR team is methodical in our approach to these cyber emergencies. First and foremost, our priority is to stop the bleeding, find out what happened, and restore systems to normal operations as soon as possible. We treat the digital environment just like a crime scene because that’s exactly what it is. And like all crimes, the perpetrators leave a trail of evidence behind that needs to be thoroughly analyzed to truly understand the scope and depth of the attack. This thoroughness ensures that the bad guys are cleared out of the environment for good and that the attack path they used is secured.

Reporting

Assura’s Managed SIEM service comes with several reporting options. Our SOC can generate the following reports out of the USMA platform:

- 33 pre-defined event reports based on the type of data source such as firewall events, endpoint security events, web server events, VPN events, etc.

- 26 pre-defined reports by specific data source such as Windows logs, AlienVault NIDS, AlienVault Agent command history, etc.
- 14 pre-defined PCI DSS compliance reports.
- 16 pre-defined NIST CSF compliance reports.
- 5 pre-defined HIPAA Security Rule compliance reports.
- 15 pre-defined ISO 27001 compliance reports.

In addition, Assura sends weekly reports of low-severity alarm activities (i.e., alarms that represent normal network activity not part of a security incident such as user account unlocks by system administrators, group membership changes made by system administrators, etc.)

Finally, Assura presents a report on prior month's activities, along with recommendations to improve the client's security posture based on the observations and expertise of the assigned SOC Concierge. The report is discussed in detail via a web conference where the SOC Concierge presents the data and trends in a live, interactive format so that your stakeholders can ask anything about the data or anything else cybersecurity related. Many of our clients use this time for us to weigh in on other security-related issues such as policy, technology, training, and compliance issues. We bring our expertise in all security domains for all clients.



2.2.3 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 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).

Before the Test

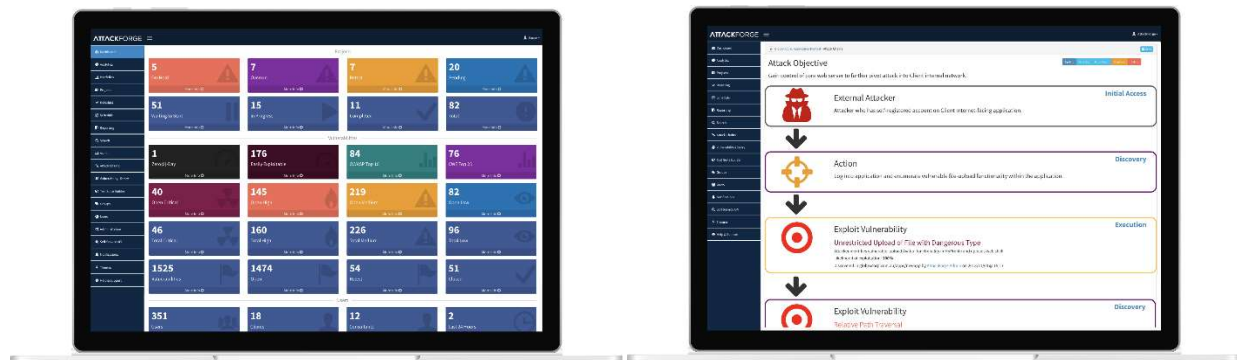
We have a conversation with the client to find out what is most important to them and discuss our process:

- Each engagement is tailored to meet their needs and concerns.
- Our tests are hands on the keyboard, human testing as opposed to hands-off tool scanning, or black, gray, and white box testing.
- We discuss the threat model they are looking to emulate to ensure testing is in alignment with what your environment must defend against.
- All information is captured in the Rules of Engagement, which guide how the test is to be conducted.

During the Test

We communicate all critical vulnerabilities, concerns, and other relevant information to the organization based on the desired level of communication:

- Access to AttackForge platform:
 - Assura adds vulnerability findings for the client to review, begin remediation, and request retesting.
 - Clients have visibility into the AttackChains Assura develops to paint a picture of attack paths within the environment and view the Test Cases that penetration test team has completed.



- Access to asset data via RunZero, an asset identification and fingerprinting system:
 - Many organizations use this data to check our coverage against their asset inventory or even use this data to develop or update their own asset inventory.

Asset Inventory

Scan Import Connect Report Audit

0 selected Viewing 0 - 52 of 52 results 20 results

Address	Up	Attr	Hostname	OS	Type	Hardware	Outlier	MAC Vendor	MAC Age	MAC	OS EOL	Sources	Con
10.01.200			P53R	Fedora Linux	Server	Lenovo 20QCT0TWW	2	LCFC (HaPa) Electron...	2019-08-09	3C:07:96:07:AB:87			
192.168.0.3			OPENSENSE		Router		2	Deciso B.V.	2012-03-28	04:ED:33:C3:A3:76			
192.168.0.2			UNIFI-CLOUDKEY	Unifi Cloud Key	Network Management Device	Ubiquiti Unifi Cloud Key	3	Ubiquiti Networks In...	2014-12-17	78:02:94:2D:86:9E			
192.168.0.3			LAB-SCANNER	Ubuntu Linux	Server	VMware VM	2	VMware, Inc.		78:02:94:2D:86:9E			
192.168.0.4			TENTACULAR	Ubuntu Linux	Server		2	Intel Corporate	2011-04-29	D4:5D:64:D2:9B:A6			
192.168.0.5			DEVELOPERS-MAC-MIN	Apple macOS	Desktop	Apple Mac Mini (Late 2018)	2	Apple, Inc.	2017-12-23	D4:5D:64:D2:9B:A6			
192.168.0.6			BRV-APPROX-CONTRIN	Raspbian Linux	Server	Raspberry Pi	3	Raspberry Pi Foundat...	2012-02-11	F8:AF:CA:8E:C1:19			
192.168.0.19			RACKAPCDI	APC AP9631	UPS	APC Smart UPS Web Management Card	2	AMERICAN POWER CONVE...		00:F6:20:4E:D7:84			
192.168.0.21			S3300-SERVERROOM	Netgear S3300-28X	Switch	Netgear S3300-28X	2	NETGEAR	2018-09-23	54:88:0E:56:D3:9E			
192.168.0.21			M4300-OFFICE	Netgear S3300-28X	Switch	Netgear M4300-8XSF	2	NETGEAR	2015-12-22	3C:07:96:07:AB:87			
192.168.0.22			M4300-WORKBENCH	Netgear M4300-8XSF	Switch	Netgear M4300-8XSF	2	NETGEAR	2015-12-22	50:37:88:07:AB:77			
192.168.0.22			M4300-SERVERROOM	Netgear M4300-8XSF	Switch	Netgear M4300-8XSF	2	NETGEAR	2015-12-22	50:37:88:07:AB:77			
192.168.0.24			M4300-ADU	Netgear M4300-8XSF	Switch	Netgear M4300-8XSF	2	NETGEAR	2017-04-18	4C:07:98:07:4B:66			
192.168.0.41			DATASETS	Synology DSM	NAS	Synology NAS	2	Synology Incorporate...					
192.168.0.42				Synology DSM	NAS	Synology NAS	1	Synology Incorporate...	2021-04-01	3D:45:97:D6:3C:81			
192.168.0.53			PISDEV	Microsoft Windows 11 (Build 22H2)	Desktop	Lenovo 20YQ00IMJ5	2	LCFC (HaPa) Electron...	2021-04-01	23:3F:54:87:C1:A8			
192.168.0.60			RUMBLE-ESXi-1	VMware ESXi	Hypervisor	VMware ESXi	2	ASRock Incorporation	2018-01-26	2E:3D:77:4B:C4:E1			
192.168.0.60			RUMBLE-ESXi-1	VMware ESXi	Hypervisor	VMware ESXi	2	Super Micro Comput...	2013-10-24	2E:3D:77:4B:C4:E1			

1 2 3 4 5 6 7 ... 60

After the Test

Assura develops a report that includes all findings, steps to reproduce, recommended remediations for each vulnerability, and schedule a briefing with the team:

- Additionally, a review of the open-source information gathered about the organization, a summary of social engineering campaigns, executive summary, and our recommendations for a holistic approach to fixing issues are included.
- We meet with the organization to conduct an in-person or virtual briefing on the engagement and results targeted at technical staff, director-level, or executive and board members.
- The organization has 60 days to request retesting from Assura for every finding reported in AttackForge. After the 60 days have lapsed, Assura generates an updated penetration test report to show any progress.
- The organization has access to AttackForge for 1-year from the engagement start-date and access to RunZero for 90 days from the engagement start-date.
- Any "0-day" vulnerabilities found in commercial software within the client's environment are reported by Assura to the vendor and MITRE/the National Vulnerability Database for remediation and tracking.
- Assura adopted a responsible disclosure policy in late 2021 to assist clients with the difficulty of getting commercial software developers to fix newly found vulnerabilities. That policy and several of Assura's CVEs can be found at <https://assura.atlassian.net/wiki/spaces/VULNS/overview>

PENETRATION TEST TYPES

External Network Penetration Test

The Assura penetration testing team assigned to the engagement carries out a penetration test that aligns to a custom methodology which draws from and meets the requirements of PCI- DSS, HIPAA, NIST SP 800-115, OSSTMM, and the Pentest Standard. Depending on the needs of the client, Assura aligns testing methodologies to any regulatory, contractual, or custom requirements through the creation of custom test cases.

Stages of the External Network Penetration Test include:

- OSINT – Open-Source Intelligence Gathering takes three primary forms as part of an evolutionary process – passive, semi-passive, and active. The purpose of OSINT is to help paint the picture of what the organization does, who works there, what technology is in place, what service providers and business partners exist, etc. to gain insight into the best avenues of attack.
- Footprinting – In this stage, Assura is focused on gathering information about the IP range and/or DNS names available for attack. Activities include “whois” lookups, BGP looking glass reconnaissance, port scanning, DNS brute forcing, enumeration of services and versions, mapping web sites, and initial identification of potential vulnerabilities.
- Vulnerability Analysis – Assura utilizes automated vulnerability scanning tools such as Nmap's scripting engine, Nessus Professional, Invicti, WPScan, etc. to identify what we generally refer to as “low hanging fruit”. Those are the vulnerabilities which are easily identifiable by an adversary with limited resources and skills. This information is used as input into furthering our manual penetration testing.
- Manual Assessment and Exploitation – At this stage, Assura's penetration testers focus on the specific services which may be vulnerable to attacks based on the information gathered in previous stages. Manual assessment may include traffic inspection and manipulation in tools such as BurpSuite or via Wireshark for non-web protocols. From there, Assura develops custom test cases and exploits to demonstrate the impact of the vulnerability in your environment. All steps to reproduce the exploit are included in AttackForge and the formal report.

Internal Network Penetration Test

The Assura penetration testing team assigned to the engagement executes a penetration test that aligns to a custom methodology which draws from and meets the requirements of PCI- DSS, HIPAA, NIST SP 800-115, OSSTMM, and the Pentest Standard. Depending on the needs of the client, Assura will align testing methodologies to any regulatory, contractual, or custom requirements through the creation of custom test cases.

Stages of the Internal Network Penetration Test include:

- Logistics – Due to the sensitive nature of internal networks, Assura works with the client to determine what systems are in-scope for testing and what systems should be tested but considered “fragile”. Additionally, Assura works with the client to determine lockout policies to avoid user experience issues and ensure that the penetration test team is covering all areas of the network desired by the client.
- Enumeration – In this stage, Assura is focused on gathering information about the IP range and Domain through LDAP reconnaissance, packet captures, port scanning, DNS reconnaissance and brute forcing, enumeration of services and versions, mapping internal web sites, and initial identification of potential vulnerabilities.
- Vulnerability Analysis – Assura utilizes automated vulnerability scanning tools such as Nmap's scripting engine, Nessus Professional, BurpSuite Professional, WPScan, etc. to identify what we generally refer to as “low hanging fruit”. Those are the vulnerabilities which are easily identifiable by an adversary with limited resources and skills. This information is used as input into furthering our manual penetration testing.

- Manual Assessment and Exploitation – At this stage, Assura’s penetration testers focus on the specific services which may be vulnerable to attacks based on the information gathered in previous stages. Manual assessment may include traffic inspection and manipulation in tools such as BurpSuite or via Wireshark for non-web protocols. From there, Assura develops custom test cases and exploits to demonstrate the impact of the vulnerability in the context of your environment. All steps to reproduce the exploit are included in AttackForge and the formal report.

Web Application/API Penetration Testing

The Assura penetration testing team assigned to the engagement carries out a penetration test that aligns to a custom methodology which draws from and meets the requirements of PCI- DSS, HIPAA, NIST SP 800-115, OSSTMM, and the Pentest Standard. *Specifically, for Web Application/API Penetration Tests, Assura utilizes the OWASP Application Security Verification Standards to ensure adequate test case coverage.* Depending on the needs of the client, Assura aligns testing methodologies to any regulatory, contractual, or custom requirements through the creation of custom test cases.

- Reconnaissance – Based on the scope of the penetration test, Assura’s penetration testers gather the necessary information about the target web application(s). This includes URLs, descriptions/documentation about application logic, business use-cases, infrastructure, and application technology stacks in use. The penetration testers also ensure that they have adequate access to the system from an authentication and network reachability standpoint.
- Logic Assessment – The penetration test team manually examines and uses the application to better understand the intended uses of the application. It is only based on a thorough understanding of what an application *should* do that a tester can then develop custom test cases to determine if the application takes actions or responds to the tester in a way that it *should not*.
- Automated Crawling – The penetration test team uses the information gathered during the logic assessment phase to further “crawl” the system to find pages that were not previously discovered. Additionally, the testers use a technique called “brute forcing” to find hidden directories and pages which may not be discovered simply through crawling.
- Automated Vulnerability Scanning – The penetration test team utilizes tools such as Invicti, BurpSuite Professional, SQLmap, XSSStrike, and Nikto to discover vulnerabilities that would be considered “low hanging fruit”. Those are the vulnerabilities that would be easily discovered by an attacker with limited skills and resources at their disposal.
- Manual Assessment and Exploitation - At this stage, Assura’s penetration testers focus on the completion of the OWASP Test Suites based on the OWASP Top 10 and ASVS. From there, Assura develops custom test cases and exploits to demonstrate the impact of the vulnerability in the context of your environment. All steps to reproduce the exploit are included in AttackForge and the formal report.
- Additional Insights into OWASP Test Suites:
 - For 2017, the OWASP Top 10 Most Critical Web Application Security Risks (in the Release Candidate) are:
 - A1 Injection
 - A2 Broken Authentication and Session Management
 - A3 Cross-Site Scripting (XSS)
 - A4 Broken Access Control (As it was in 2004)
 - A5 Security Misconfiguration
 - A6 Sensitive Data Exposure
 - A7 Insufficient Attack Protection (New)
 - A8 Cross-Site Request Forgery (CSRF)
 - A9 Using Components with Known Vulnerabilities
 - A10 Under protected APIs (New)

- For 2013, the OWASP Top 10 Most Critical Web Application Security Risks are:
 - A1 Injection
 - A2 Broken Authentication and Session Management
 - A3 Cross-Site Scripting (XSS)
 - A4 Insecure Direct Object References
 - A5 Security Misconfiguration
 - A6 Sensitive Data Exposure
 - A7 Missing Function Level Access Control
 - A8 Cross-Site Request Forgery (CSRF)
 - A9 Using Components with Known Vulnerabilities
 - A10 Unvalidated Redirects and Forwards
- ASVS
 - V1. Architecture, design, and threat modelling
 - V2. Authentication
 - V3. Session management
 - V4. Access control
 - V5. Malicious input handling
 - V7. Cryptography at rest
 - V8. Error handling and logging
 - V9. Data protection
 - V10. Communications
 - V11. HTTP security configuration
 - V13. Malicious controls
 - V15. Business logic
 - V16. File and resources
 - V17. Mobile
 - V18. Web services (New for 3.0)
 - V19. Configuration (New for 3.0)
- ASVS API
 - Protocols for Authentication and Authorization
 - REST services are stateless
 - Access Control
 - Input validation
 - Output encoding
 - Cryptography
 - Message Integrity
 - Confidentiality
 - HTTP Return Code
 - Improper Data Sanitization
 - Insecure Direct Object Reference
 - Insufficient Transport Layer Security
 - Sensitive Data Exposure
 - Weak Server-Side Security
 - Improper Key Handling
 - Inconsistent API Functionality
 - Security Misconfiguration

Wi-Fi Penetration Testing

Assura's Wi-Fi penetration tests ensure that your organization is utilizing best practices for Wi-Fi security such as the latest encryption technology, strong passwords, and adequate network segmentation.

- Reconnaissance – Assura reviews the SSIDs in scope, discovers any additional or hidden SSIDs, then identifies the Wi-Fi protocols in use to determine the applicable attacks.
- Exploitation – Assura utilizes techniques to obtain pre-shared keys for “cracking” to obtain plain text passwords. This includes:
 - De-auth attacks
 - PMKID capture
 - Rouge Access Point
 - WPS brute force attacks and “pixie dust” attacks
 - Username Capture and EAP-Brute forcing for WPA Enterprise environments

If Assura is then able to access the network after obtaining the pre-shared key, Assura validates that the Wi-Fi network is appropriately segmented from other networks based on the SSID’s intended use-case. Specifically, we ensure that the guest network (if in place) cannot be used to access sensitive networks.

Cloud Penetration Test and Cloud Conformity Audit

Assura’s Cloud Penetration Tests and Cloud Conformity Audits are based on the application of traditional penetration testing techniques combined with Trend Micro’s Cloud Conformity Standards which contain 750+ best practices for your AWS, Microsoft Azure, and Google Cloud environments. The client receives a thorough understanding of how exposed their cloud environment is to attacks and what configuration changes the organization can make to better fortify that environment against future attack.

- Reconnaissance – Assura reviews any initially provided documentation and reviews the scope of the Cloud environment to ensure adequate coverage. Assura performs external scope discovery exercises to reveal the publicly available attack surface such as Virtual Machines, Storage, APIs, Authentication points, etc. This step ensures that we ensure that we have identified the potential attack surface, which also verifies that we have adequate access during the audit.
- Component Enumeration – At this phase, the Assura penetration tester assigned to perform the Cloud Conformity Standards audit authenticates to the environment using the provided credentials. The tester then gets acclimated to the environment and determines which test cases within the Cloud audit are applicable.
- Automated Component Configuration Review – Optionally, Assura can utilize Tenable.io to conduct a Cloud Configuration review based on CIS best practices. This step is only performed based on the client’s desire to have their environment scanned in addition to the manual audit.
- Manual Assessment and Configuration Review – Assura’s penetration testers utilize the Cloud Conformity Standards to identify weak security configurations and recommend enhancements. The team also attempts to exploit potential vulnerabilities in the services discovered during reconnaissance to demonstrate the impact and tie that finding back to the standard.
- Architectural Design and Custom Test Cases Review – It is not uncommon that once we are inside of a client’s environment, we discover service integrations or configurations that may not be covered by any automated scan or audit standard. When Assura’s penetration test team encounter a unique design concept or see a potentially misconfigured integration, we work with the client’s team to determine the impact and report this accordingly.

Physical Security Assessment

Assura can conduct physical security assessment from the perspective of a knowledgeable insider where we openly work with the client’s team to identify weaknesses in physical security controls, or the test can be performed from the perspective of a true attacker with a goal in mind. Assura works with the client to determine the needs of the organization and develop a scope based on that conversation.

- Reconnaissance – The penetration tester reviews the scope of the assessment and determines what information they need to research. This could lead to them taking actions such as looking up building records, local laws, and regulations to learn about physical security, review the organization and its employee’s social media to see what badges look like, reviewing what the inside of the building looks like, and determines what security controls they should expect to

encounter, etc.

- Preparation – The penetration tester develops with their intended ploy to access the building to achieve their objective, whether that be installing a remote access device on the network, accessing the MDF closet, or getting into your office to obtain a “flag”.
- Execution – If the engagement is being performed as more of an audit than a test, the tester arrives on site and walks through the building with an employee to test and identify physical security control gaps and areas for improvement. If the engagement is being performed to mimic a real-world threat, the penetration tester communicates with the client to determine an appropriate window for test execution. This may include deploying the following tactics:
 - Implementation of badge cloning technology
 - Fake ID cards
 - Social engineering
 - Physical control bypass such as “slipping” a lock
 - Tailgating

Social Engineering

Assura can develop social engineering campaigns to meet all needs. The focus of social engineering at Assura is not to shame users who fall victim, but to identify where weaknesses in user training and policy are and help the organization to develop better practices and effective training materials. We custom tailor social engineering engagements using the following methods:

- Phishing – targeted spear phishing campaigns and/or mass-emailing attacks.
- Vishing – Voice based phishing via a telephone to obtain information that should otherwise be confidential.
- USB Drops – Assura drops USB keys in conspicuous locations around your facilities to see which users pick them up and plug them into their device.
- Social Media – LinkedIn and other social media platforms are great ways to infiltrate your organization. Assura develops fake personas to see if your employees provide too much information or violate security practices.
- In-Person – Paired with a physical assessment, Assura comes on-site to determine if testers can gain access to sensitive areas or information.



2.2.4 Vulnerability Management-as-a-Service (VMaaS)

One of the most common means that threat actors use to compromise an organization's security is taking advantage of systems with lingering security flaws and weak configurations. With Assura's Vulnerability Management-as-a-Service, we take a risk-based approach to keep the bad guys from finding and exploiting those weaknesses, prioritizing the vulnerabilities that matter the most.

VMaaS includes ongoing vulnerability scans, detailed vulnerability reports, a guided explanation of what it all means, and more. Each VMaaS client is assigned a dedicated service concierge from our Offensive Security Operations team. Our expert will facilitate a monthly conference to highlight trends and make treatment recommendations for the client. These added insights provide the client with an "attacker's eye view" of their attack surface.

Assura's VMaaS service utilizes tools such as Tenable Nessus, Beagle application scanning, 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 VMaaS service not only uncovers security flaws from outdated software, but it also uncovers 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.

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.

All vulnerabilities are ingested and reported into Nucleus, a cloud-based vulnerability intelligence and management platform. Nucleus automatically enriches all vulnerability data using enterprise class vulnerability and threat intelligence powered by Mandiant. By combining the aggregation, analytics, and vulnerability management orchestration capabilities already provided within Nucleus with the insight and intelligence provided from the Mandiant team, practitioners can accelerate the vulnerability prioritization and triage process using automation at scale and have the data they need to rapidly make confident decisions and accurately assess the risk of vulnerabilities. Nucleus combines all the asset information, vulnerability data from scanning tools, and threat intelligence into one single platform for vulnerability teams to eliminate laborious manual data analysis, accelerate decision-making and prioritization, and remove major pain points that exist for all organizations trying to mature their vulnerability management programs.



In a single pane of glass, Nucleus correlates all organizational asset information, vulnerability data from network, application, cloud and container scanning tools, org charts, system hierarchies, and three complete feeds of vulnerability intelligence so practitioners can assess what matters most. Nucleus normalizes the data enabling teams to evaluate, triage, prioritize, and remediate much faster with greater precision.

Assura's OSO Concierge works with the client to fully configure and customize Nucleus, set up all integrations and workflows, determine remediation priorities, and train the client on its use.

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.



2.2.5 Multifactor Authentication (MFA)

Assura implements Duo, the world's leading identity security platform seamlessly into the client's environment. But that's just the beginning. We also make sure that MFA is aligned with any associated program policies and procedures. Or if there isn't a program in place and one is needed, we provide that for the client. Our goal is to deliver a complete solution that secures user access and adheres to compliance requirements, avoiding any potential regulatory issues down the road is a top priority.

Tech Specs of Assura's MFA Solution:

- Enhanced security for modern and legacy applications.
- Support for Outlook Web App, VPN services, Office 365, G Suite, Amazon Web Services, Windows Workstation Access, WordPress, Salesforce, and others.
- Synchronization with the existing user management platform.
- Enforces conditional access to sensitive applications.
- Restricts access based on geolocation.
- Supports a wide variety of authentication methods, including push notifications to smartphones (iOS and Android), Universal 2nd Factor (U2F) tokens, one-time passwords, and phone callbacks.
- Satisfies the multifactor authentication requirements of PCI DSS, NIST SP 800-171, FFIEC, and more.



2.2.6 ProDefense

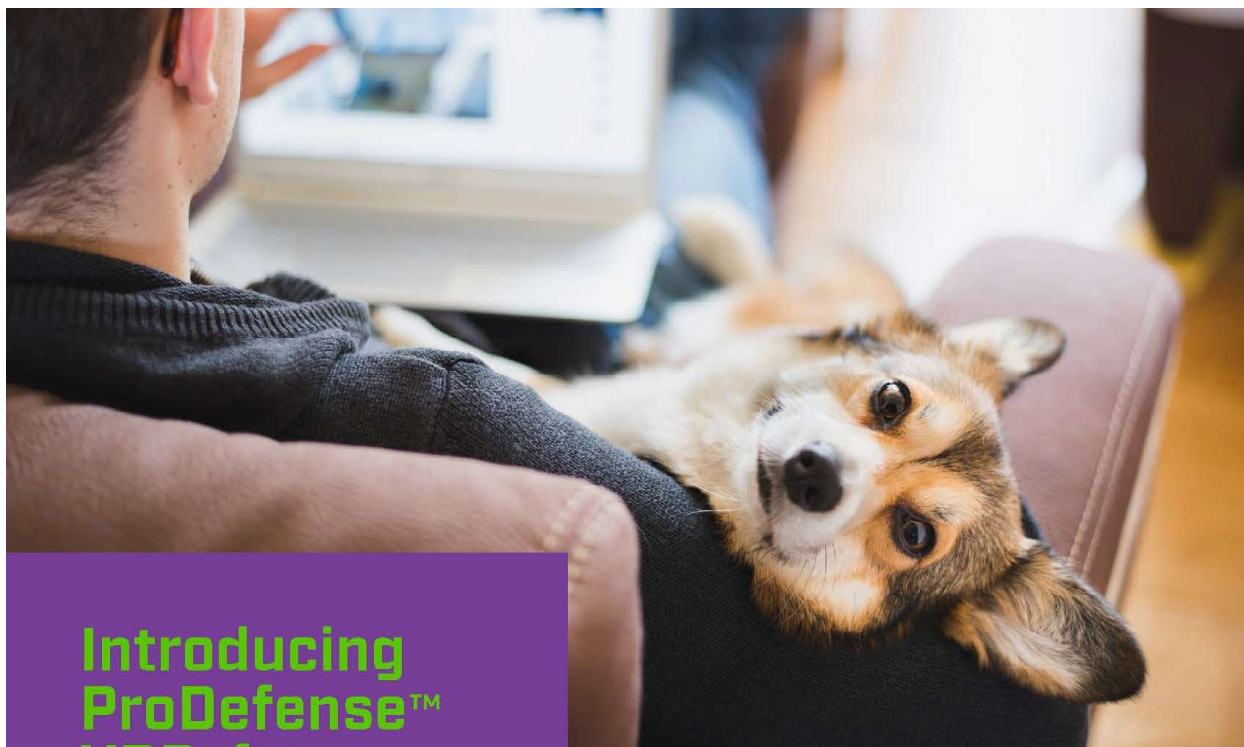
ProDefense XDR is a security-forward end user computing lifecycle management solution that protects systems using the latest tools and technologies and delivers guaranteed compliance with any cybersecurity framework. Operated by our Security Operations Center and backed by our AuditArmor® Guarantee, ProDefense XDR is the right solution for organizations that want to put the power of a secure computing platform into the hands of their users to facilitate use cases such as work-from-anywhere, virtual call center, public safety dispatch, mobile data terminals, and many more!

ProDefense uses off-the-shelf Microsoft Windows 10/11, Apple macOS, Apple iOS, or Google Android devices in combination with secure cloud-based services to centrally control and enforce device configurations, deliver security updates, monitor device health, and monitor device security posture. Each device runs with lightweight agents that work in harmony to defend against the latest cyberattacks without slowing down device performance.

ProDefense enrolled assets can defend against attacks whether or not they are connected to a network or the Internet.

ProDefense XDR is available for Academic, Commercial, Government Compute Cloud (GCC), and GCC High use cases and comes with the following features and functions (see the chart below for detail about plans and features):

- Secure “over-the-air” deployment and configuration – no more managing gold loads or imaging systems.
- Secure “over-the-air” deployment of applications.
- Next Generation (NextGen) behavior-based antivirus and Endpoint Detection and Response (EDR) using the latest advanced Machine Learning (ML) models.
- Transparent storage encryption.
- Device level firewall.
- Security activity logging and telemetry.
- Multifactor authentication.
- Web content filtering with an optional permit-by-exception operational model.
- Optional application whitelisting.
- Optional direct application installation for authorized power users.
- Remote asset wipe.
- Stolen device protection.
- Advanced AI-driven email security.
- Awareness and training for end users to ensure that the “human firewall” is active.



Introducing ProDefense™ XDR, for today's virtual workplace.

What is ProDefense XDR?

- A robust Windows PC deployment and Extended Detection and Response (XDR) solution
- Provides infinite scalability, control, visibility and compliance for a variety of use cases
- All cloud-based platform delivers security anywhere in the world
- Provides configuration control, threat blocking, threat detection, URL/content control, and continuous monitoring

Does ProDefense XDR make sense for your business?

Whether your employees work on-site, remotely or a combination of both, the answer is yes. ProDefense XDR delivers quick security and compliance that broadens your ability to make work from anywhere work for your business.

What this means for your business:

- You can safely expand your talent pool outside your geographic area
- Frees up your IT staff to focus on strategy and the day-to-day demands of the business
- Productivity never suffers because an employee can be up and running in as little as twenty minutes on a new, secure system
- End users never have to connect through a VPN

ProDefense™ XDR Plans

BASIC

ADVANCED

ULTIMATE

FEATURES

PLANS

Next Generation AI-based antivirus and Endpoint Detection and Response (EDR), ransomware rollback, forensic investigation, and threat intelligence

Persistent foothold detection and eradication

Logging and monitoring with File Integrity Monitoring, malware and web shell detection, user behavior analytics, and basic forensic analysis

Windows 10 Enterprise for the most advanced security features

Provision-from-anywhere deployments (no more "gold loads")

Touchless deployments

Configuration compliance with any security standard

Configuration compliance enforcement

Application deployment and corporate app store

FEATURES

PLANS

User Account Management in Microsoft Azure Active Directory or hybrid Active Directory deployment

Cloud Application Security

Data Loss Prevention (DLP)

Patch Management

Vulnerability Identification and Management

Multifactor Authentication

URL and Content Filtering

Office 365 Add-on Available

iOS and Android Mobile Device Management (MDM) Add-on Available

Advanced Artificial Intelligence Driven Email Security

Security Awareness & Training Program



2.2.7 Advisory Services

While Assura endeavors to create managed service solutions that meet every client's needs; there are instances where customized solutions are required. Advisory services are project based and cover just some of the following areas:

- IT and Cybersecurity Strategic Planning
- Network Engineering and System Integration
- Help Desk Support
- Cybersecurity System Engineering and Implementation
- Program Roadmaps
- Program and System Risk Assessment
- Supplier/3rd Party Risk Assessment
- System Security Plans
- Business Impact Analysis (BIA)
- Role-Based Training
- Continuity and Disaster Recovery Planning
- Security Audit Defense
- Dark Web Threat Intelligence

Assura will work with the client to individually scope and price Advisory Services projects.

2.2.8 Security Life Cycle for Amazon Web Services

Assura is an Amazon Web Services (AWS) Validated partner with expertise in helping clients ensure that when they migrate workloads into AWS they are doing so in a way that ensures security and compliance.

We help clients do this in the following ways:

- Ensuring adequate governance, risk, and compliance activities are conducted with the creation of artifacts that ensure traceability and assurance.
- Assisting clients to implement the Security Pillar of the AWS Well Architected Framework.
- Federated identity management with services such as AWS Cognito.
- Conducting vulnerability assessments and management using AWS Inspector, Systems Manager, and other tools.
- Conducting penetration tests to assess the effectiveness of protective, detective, and corrective controls.
- Monitoring, hunting for, and investigating threat activities using CloudTrail, CloudWatch, GuardDuty, VPC flow logs, and other mechanisms.
- Conducting breach investigations and forensic analysis.
- Designing and implementing backup, archiving, and disaster recovery solutions built in AWS using services such as AWS Backup, Glacier, and Elastic Disaster Recovery.

Assura offers clients the option of using their own AWS subscriptions with negotiated pricing or purchasing through Assura.

2.3 Personnel

RFP Requirement: “IV.3 Provide the names, qualifications, and experience of personnel to be assigned to James Madison University. Designate who would be assigned as the primary contact for the account.”

Assura was doing cybersecurity before it was “cool”. The company was started in 2007 by our CEO, Karen Cole, a seasoned executive who at one time was in charge of global disaster recovery for Capital One; and our CTO Joshua Cole, a cybersecurity industry veteran with deep experience in the software, defense, and intelligence communities with companies such as Hughes Aircraft (now Raytheon), EDS (now NTT), and Booz Allen Hamilton. Assura is located in Richmond, Virginia but provides cybersecurity services to clients across the United States and Canada.

The firm started as a professional services consultancy assisting Virginia state universities, colleges, state agencies, local governments, banks, healthcare, manufacturing, and other industries with one mission: secure the future one client at a time by providing the most customer-centered focus in the industry. We’re proud that we live up to that promise and our clients represent most consistent source of referrals for new business.

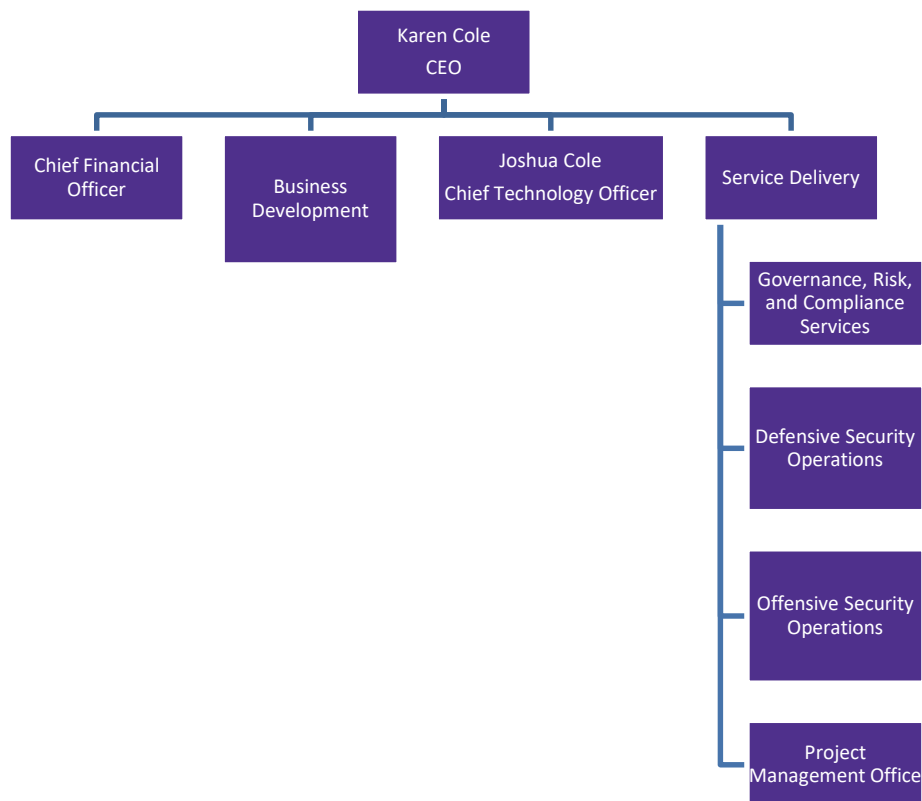


Figure 1 - Assura, Inc. Organizational Structure

While we still perform advisory projects for many clients and which is included in our proposal, we have also expanded our offerings to encompass managed security services. Throughout its history, clients asked Assura to start its own Managed Security Services Provider (MSSP) offerings to fill the gap for organizations that did not need or have the resources for an information security department, but needed Governance, Risk, and Compliance (GRC) services that integrated with other managed services such as Managed Security Operations Center (SOC) services.

With respect to the reviewers of this proposal and in trying to meet the spirit of limiting this documentation size of this proposal, we are providing an overview of top executive of the firm who will ensure that quality

standards are met, as well as allocating resources to meet our commitments. However, we are happy to provide resumes for other personnel upon request.

Karen Cole

CBCP, CISA, CRISC, MBCI, CMMC RP

Chief Executive Officer



Areas of Expertise

- Governance, Risk, and Compliance Planning and Executive Leadership
- Continuity Planning
- Audit and Assurance Planning
- Business Strategy and Operations

Overview

Ms. Cole is the CEO and Board Chair of Assura, Inc., a certified woman owned company. She is an expert in the areas of information security, continuity planning and risk management, as well as governance, risk, and compliance. She is a seasoned Information Technology solutions practitioner and auditor with extensive experience in various technical risk management disciplines including Information Security, Privacy, Disaster Recovery, Business Continuity/Continuity of Operations/Continuity of Government, Crisis Management, and Internal Controls. She is an industry expert for NIST 800-53, NIST 800-34, ISO 27000 and 31000, PCI-DSS, CJIS, FFIEC, FDICIA, Gramm-Leach Bliley Act, and FDIC compliance for information technology organizations. Ms. Cole has the ability to initiate/implement crucial business development and operational strategies; recruit/develop multi-disciplinary teams and achieve significant results. She also has excellent negotiating, communication, and interpersonal skills at all levels.

Professional Experience

Assura Inc. Chief Executive Officer, 2007-Present

- Provides strategic direction and executive oversight for the firm and ensures adherence to all business, quality, and ethical standards.
- Leads numerous engagements to develop and implement risk management programs for numerous public and private sector clients that result in regulatory compliance and improved business operations.
- Designs and implements business continuity, crisis management, disaster recover, Continuity of Government and Continuity of Operations Plans for several private and public sector clients.
- Implements various information security programs to meet the requirements of many different security frameworks including NIST, ISO, CMMC, HIPPA, GDPR, and more.

Joshua Cole

CISM

Chief Technology Officer



Areas of Expertise

- Business Strategy and Operations
- Governance, Risk, and Compliance
- Defensive Security Operations
- Attack Tactics
- Forensics

Overview

Mr. Cole is the Chief Technology Officer for Assura Inc. With 25 years of experience, Mr. Cole is constantly developing new skills in technology and has a knowledge base in: Microsoft, Cisco, Apple, and Linux products; TCP/IP; LAN/WAN; risk assessment; intrusion detection; vulnerability assessment; penetration testing; identity management; firewalls; VPNs; Public Key Infrastructure (PKI); 802.11 Wireless LAN; application security; mobile communications; and encryption algorithms. Throughout his years in the field, Mr. Cole has proven himself as a leader by managing complex projects that resulted in improved strategic and operational outcomes that were both delivered on time and on budget.

Professional Experience

Assura Inc. Chief Technology Officer, 2014-Present

- Responsible for overseeing the development and implementation of new and innovative products and services to help Assura's clients solve difficult governance, risk, and compliances as well as technical cybersecurity challenges.
- Oversees Assura's Managed Security, Penetration Testing, Digital Forensics, and Investigation (DFIR) services, and corporate information technology.
- Executes high complexity and high-risk special projects for Assura clients.

Assura Inc. Executive Vice President, Sales/ Marketing, 2013-2014

- Led capture of new business with small, mid-sized and large public and private-sector clients including capture strategies and proposal development.
- Cultivated strategic alliances and partnerships to bring new capabilities and opportunities to the company resulting in opportunities with multimillion-dollar Department of Defense programs.

Assura Inc. Chief Operating Officer, 2007-2013

- Led the successful development and implementation of cybersecurity program strategies and frameworks in compliance with federal, state, and industry standards.
- Invented Calibrated Risk Index® (CRI), a methodology to both measure risk quantitatively and qualitatively in a single metric; and tie risk directly to compliance.

From an individual performer standpoint, Assura provides a primary and a secondary resource (called "Concierges" for our Security Monitoring and Vulnerability Management services) for each service purchased to ensure high levels of service continuity and client satisfaction. Supporting resources are

assigned to the client after an initial intake interview is performed by Assura's Project Manager or a Concierge to determine the best resource to meet the client's needs.

All staff are background checked for criminal history in all 50 states and the District of Columbia, sex offender registries, driving record, SSN trace, address, DOB, and name verification. Depending on the client need, we will also include a credit and financial health check. For certain positions, we also conduct a full education verification.

All current Assura employees are citizens of the United States of America.

2.4 Consultants Continuity Plan

As a firm that performs disaster recovery and resilience planning, continuity is a core component of our operations. For each engagement, there are three levels of contingency resources that are assigned.

Principal Consultant

The Principal Consultant is responsible for project oversight, providing executive program leadership, and ensuring continuity of services provided to the client throughout the project. When needed, the Principal Consultant will provide direct services if the Senior Consultant and Consultant are not available.



Senior Consultant

The Senior Consultant is an experienced practitioner who is responsible for working with the consultant to validate approaches, strategies, and deliverables. When needed, the Senior Consultant will provide direct services if the Consultant is not available.



Consultant

The Consultant has a significant amount of experience in their respective service areas before being authorized to provide direct services to a client. Additionally, all consultants maintain one or more industry certifications in their specialized field.



2.5 Available Services

Available services have been detailed in Section 2.0 of this proposal. Assura will work with JMU, the VASCUPP member organizations, and contract users to determine specific scope of services respective to those services. Pricing for these services will be in alignment with the proposed cost and pricing schedule in Section 6.0 of this proposal.

2.6 Training and Documentation

Assura provides a full suite of services to establish a “security culture” that is welcoming of the Information Security and Information Technology Program efforts and that is supportive of its activities.

Value

A majority of data breaches caused by human error; therefore, training and awareness programs are more than just the add-on at the end of program implementation - they are a critical success factor for program effectiveness. These programs provide the mechanism for ongoing communication with an Information Security Program’s clients/users and is critical for obtaining their buy-in for program participation, gathering information on security incidents as well as current risks/issues, and finally recommendations needed adjustments or improvements.

Approach and Methodology

The training and approach methodology will change depending on the needs of the client and are determined based upon some of the following:

- Integration with current training and awareness programs (planning work will be performed to ensure full integration with existing training structures/process).
- Existing marketing and communication mechanisms to students, employees, vendors, and stakeholders that can be leveraged to reduce level of effort and cost for the organization.
- Utilization of technologies to provide “teachable moments” for individuals who unknowingly click on unauthorized links or attempt to access unauthorized data.
- Leadership direction for utilization of in-person training and awareness activities verses computer-based-training.



Listed below are some of the major training program deliverables. The exact listing of training materials is determined during scope discussions with the organization.

- Training policies and procedures
- Training curriculums
- Instructor guides
- Training materials (including presentations, student guides, tests/quizzes)
- Security awareness campaigns (ex. Awareness posters; educational emails, social media campaigns, security awareness promotion events for employees)
- KPIs for security training and awareness to support program reporting

Training Options

Assura performs several types of training to address the educational needs of the clients. Assura's principals, within our advisory services area, teach at the college level and ensure that training follows industry best practices and is right sized for the student. Listed below are some of the most popular types of training provided:

- End user training (in person or as Computer Based Training);
- Cloud services training for executives and technicians;
- Executive information security management training;
- Business Representative Training (i.e. also identified as System/Data Owner or accountable business representatives for system security);
- System Administrator;
- Data Custodian (i.e. Data center management staff or vendors responsible for physical control of systems); and
- Topic specific training (ex. Security breach incident response; dealing with cyber harassment); and
- Exercises to validate newly developed capabilities of students.

We are happy to discuss the training needs with JMU, VASCUPP members, and authorized contract users directly to ensure that the proposed training specifically addresses the organization's educational needs.

2.7 Recent Projects

Please note that per § 2.2-3700 et. seq. of the Code of Virginia, all information underlined in this section are trade secrets as defined under the Uniform Trade Secrets Acts and are proprietary and confidential to Assura and may not be released without the express written consent of Assura. This information is vital to Assura's competitive advantage and unauthorized disclosure would cause irreparable harm to Assura.

This section details three projects Assura has performed for clients. Please note that due to the sensitivity of some projects, they are protected from Freedom of Information Act requests as it would pose a security risk to their organization. However, we have been authorized to share the information directly with James Madison University. We are happy to provide this information to any VASCUPP member institution or authorized contract user directly upon execution of a non-disclosure agreement.

<u>REDACTED</u>		

REDACTED		

REDACTED		

2.8 Knowledge Transfer

Assura will provide knowledge transfer to the accountable representative(s) from the organization that is responsible for managing all follow up activities as a result from work performed during the project. It is strongly recommended that these individuals observe and/or participate in planning and deliverable development activities when possible. This will allow them the opportunity to obtain a better understanding of the program and how the deliverables are utilized. In addition, Assura will hold review sessions with client representatives to discuss the deliverables and ensure that they understand the content as well as the management and maintenance activities going forward. These activities can include training and exercises or ongoing management of identified risks.

During the Project Close, Assura will work with the organization to review any open items or issues and ensure that they understand and agree with activities to remediate these items. Assura will also work to document lessons learned with the organization and ensure that they have all final deliverables (and they have been reviewed with them).

Lastly, once an organization is an Assura client, they are considered a client for life. If at any time the client has questions regarding our deliverables or the services provided, they can contact Assura and receive support free of charge.



2.9 Project Management

Assura executes all projects in accordance with the Project Management Institute's Project Management Body of Knowledge (PMBOK). As such, each project is assigned a certified Project Management Professional (PMP) who ensures proper project initiation, planning, execution, monitoring and control, and closeout. This is illustrated in Figure 3.

Project initiation begins with an executed contract between Assura and our client that acts as authorization to begin the project.

The Planning phase includes development of a detailed project schedule, the project reporting and process, and conducting an internal kick-off meeting of the Assura project team. The purpose of the internal kick-off meeting is to ensure that all team members have a clear understanding of the scope, goals and objectives of the project as well as key milestones, dates and logistical information.

Next is the Execution phase. In this phase, the project will be executed in accordance with the methodology and approach described in the "Approach and Methodology" section above. This includes coordinating people and resources to carry out the project as well as managing project logistics.

In the Monitoring and Control phase, the Project Manager tracks and reports progress against schedule and budget to the Assura Program Manager, identifies risks and issues, and works with the project team and Program Manager to develop corrective actions (as required).

Finally, in the Closeout phase all project activities are concluded and all project documentation is finalized. Assura will work with the organization to ensure that all milestones of the project have been completed successfully and that they are satisfied with the project outcome. Any outstanding issues or action items not addressed by this project will be transferred to the organization for further management. A formal project closeout meeting will be held with the project sponsor as well as any key stakeholders to review the project outcomes and ensure that they meet or exceed the organization's expectations.

As a continuous improvement organization, Assura conducts internal After-Action Reviews of all projects to identify and incorporate lessons learned into its project methodologies and deliverables.

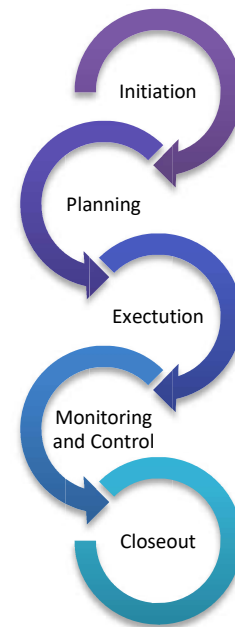


Figure 2: Assura's Project Management Approach

2.10 Functional Staffing

The functional staffing plan will be established during the services scope development process. The client organization will have the ability to review and approve all assigned resources. As detailed in Section 2.4, Assura will ensure full continuity of assigned project staff prior to the engagement.

2.11 Subcontracting Plan

Whenever possible, all information security and information technology work will be directly performed by Assura, Inc. If Assura must utilize subcontractors, we will:

- Provide awareness to the organization on the utilization of these resources and gain approval prior to engagement.
- Ensure that the selected resource is competent, and the organization properly vetted to ensure success of the project.
- Maintains industry certifications as needed.
- Whenever possible, prioritize the utilization of fellow SWaM organizations to provide services.

3.0 Attachment A: Offeror Data Sheet

REDACTED

4.0 Attachment B: Small Business Contracting Plan

ATTACHMENT B

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

Offeror Name: Assura, Inc. Preparer Name: Karen L. Cole

Date: August 15, 2023

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: 4/28/2020 to 4/28/2025

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: 4/28/2020 to 4/28/2025

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: 4/28/2020 to 4/28/2025

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 SBSB 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 Consulting Services

Date Form Completed: 8/15/2023

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

Offeror / Proposer:

Assura, Inc.

Firm

7330 Staples Mill Road, #292, Richmond, VA 23228

Address

Karen Cole, 804-672-8714

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)
N/A Assura is SWaM and DBE 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

5.0 Sales with VASCUPP Member Organizations

Please note that per § 2.2-3700 et. seq. of the Code of Virginia, all information underlined in this section are trade secrets as defined under the Uniform Trade Secrets Acts and are proprietary and confidential to Assura and may not be released without the express written consent of Assura. This information is vital to Assura's competitive advantage and unauthorized disclosure would cause irreparable harm to Assura.

The following section provides not only an overview of VASCUPP members that have utilized Assura services, but also all organizations that have benefited from this contract and its cooperative procurement component. We sincerely appreciate the opportunity to provide services to these clients using the existing VASCUPP contract for Information Technology Consulting Services.

VASCUPP Direct Member Client Spend Over the Previous 12 Months

<u>REDACTED</u>				

Additional Contract Spend for Virginia Organizations Using Existing Contract Vehicle (Not VASCUPP Member Organizations)

Client	Agreement/ Project	Start Date	End Date	Amount
<u>REDACTED</u>				

Client	Agreement/ Project	Start Date	End Date	Amount

6.0 Proposed Pricing Schedule

Virtual Information Security Officer (Virtual ISO)

Pricing for Virtual ISO services is based upon three factors discussed with the client:

1. Any upcoming or urgent information technology and security goals and/or compliance deadlines.
2. Current program artifacts in existence that can be leveraged to reduce the amount of work for the client.
3. The required timing for all program artifacts to be completed.

Once this information is determined with the client, Assura will identify the necessary resources and experience needed to perform services and the amount of time required to complete the work.

Service contracts are signed on an annual basis and billed at a flat monthly rate to be both budget friendly and predictable. All planning activities addressing compliance requirements and or deadlines will be prioritized to the greatest extent possible without compromising work quality or professional planning practices.

Plans start at \$2,175.00. Assura is pleased to offer the University a starting discount of 10% off of all Virtual ISO plans.

Security Monitoring and Response

For the Security Monitoring and Response requirement, Assura is proposing its Managed Security Incident and Event Management (SIEM) service. Our Managed SIEM service is geared toward active defense of IT infrastructure such as servers, firewalls, switches, and cloud services (end user PCs are protected with Assura's ProDefense service).

Pricing for Managed SIEM is based on three dimensions:

- A one-time charge for initial onboarding that includes design, integration, deployment of sensors and agents, and tuning.
- Monthly pricing for event storage in the AlienVault USMA platform. Plans start at 250 GB and scale all the way to 60 TB per month (custom storage amounts beyond 60 TB per month are available). This means that Assura can monitor the smallest organizations to the largest enterprises.
- Monthly pricing based on the quantity of assets in-scope to protection.
- Monthly pricing based on the quantity of mailboxes in-scope to protection.
- Optional remote forensics.

Discounts for the University start at 5% off of Assura's price book. For *illustrative purposes*, please see the table below for sample pricing for a small environment.

Item	Quantity	Price	Discounted Price	Total Price
<u>Managed SIEM Sentry Service Onboarding – One-time</u>	<u>1</u>	<u>\$10,000.00</u>	<u>\$9,500.00</u>	<u>\$9,500.00</u>
<u>AT&T Cybersecurity USM Anywhere Tenant – 500 GB Monthly Storage – 90 Days Online Searchable Data – Cold Storage – Advanced Analytics and Reporting</u>	<u>12</u>	<u>\$1,642.50</u>	<u>\$1,560.38</u>	<u>\$18,724.56</u>
<u>Managed SIEM Sentry – Per Asset Monitoring Monthly Fee – Network Infrastructure – 51-100 Assets - 24/7/365 Investigation and Reporting SLA</u>	<u>100</u>	<u>\$2,295.00</u>	<u>\$2,180.25</u>	<u>\$26,163.00</u>
Year 1 Total				<u>\$51,525.00</u>

Digital Forensic and Incident Response

The table below shows Assura's rates for Digital Forensics and Incident Response (DFIR) projects.

Labor Category	Hourly Rate	Discounted Hourly Rate
Principal Investigator	\$400.00	\$375.00
Senior Investigator	\$375.00	\$350.00
Investigator	\$350.00	\$325.00
Junior Investigator	\$325.00	\$300.00

Additional discounts may be offered based on the scope of the project.

Amazon Web Services

Assura is pleased to offer the University up to 2% off of Amazon Web Services pricing. Pricing and discounts dependent on scope of services.

Advisory Labor

The following table contains starting discounted labor rates for non-fixed price (i.e., labor hour) advisory projects. Additional discounts may be applied based on project scope and duration.

Labor Category	Starting Discounted Rate
Analyst I	\$160.00
Analyst II	\$182.50
Analyst III	\$210.25
Analyst IV	\$250.00
Analyst V	\$263.75
Analyst VI	\$267.50
Project Manager	\$148.25
Principal Analyst/Consultant	\$285.00
Director	\$308.75
Vice President	\$332.50
C-Level Executive	\$380.00

Duo Multifactor Authentication

Pricing may be adjusted if the manufacturer changes the list price.

Duo Level	List Price	Starting Discounted Price
Duo Essentials 1-999 users	\$3.00/user/month	\$2.85/user/month
Duo Advantage 1-999 users	\$6.00/user/month	\$5.70/user/month
Duo Premier 1-999 users	\$9.00/user/month	\$8.55/user/month
Duo Essentials 1000+ users	\$3.00/user/month	\$2.70/user/month
Duo Advantage 1000+ users	\$6.00/user/month	\$5.40/user/month
Duo Premier 1000+ users	\$9.00/user/month	\$8.10/user/month

Assura also has fully managed and co-managed options for this service with starting discounts of 5% off of Assura's price book.

ProDefense

ProDefense Basic pricing consists of a one-time onboarding charge and monthly per-device pricing as follows:

Description	Price
ProDefense Basic Plan 2 1-50 Devices Monthly	\$49.95
ProDefense Basic Plan 2 251-500 Devices Monthly	\$39.95
ProDefense Basic Plan 2 101-250 Devices Monthly	\$41.95

Description	Price
ProDefense Basic Plan 2 >1000 Devices Monthly	\$33.95
ProDefense Basic Plan 2 51-100 Devices Monthly	\$44.95
ProDefense Basic Plan 2 501-1000 Devices Monthly	\$36.95
ProDefense Basic Plan 1 1-50 Devices Monthly	\$41.95
ProDefense Basic Plan 1 251-500 Devices Monthly	\$31.95
ProDefense Basic Plan 1 101-250 Devices Monthly	\$34.95
ProDefense Basic Plan 1 >1000 Devices Monthly	\$26.95
ProDefense Basic Plan 1 51-100 Devices Monthly	\$37.95
ProDefense Basic Plan 1 501-1000 Devices Monthly	\$29.95

ProDefense Advanced and Ultimate plan pricing depends on a number of factors including:

- Whether Assura or the customer supplies Microsoft cloud service licenses.
- The level of Data Loss Prevention.
- Whether Office 365 is included in the service.
- The number of smart phones and tablets included in the service.

Assura is pleased to offer the University a starting discount of 5% off of Assura's price book for ProDefense Advanced and Ultimate plans.

KnowBe4

Assura is pleased to offer the University a starting discount of 10% off of KnowBe4's MSRP on all products.

Reference: Original RFP

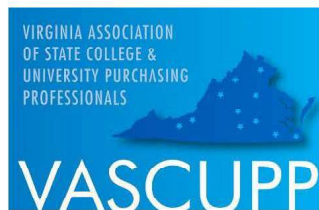


Request for Proposal

RFP# FDC-1175

Information Technology Consulting Services

June 15, 2023



DEADLINE FOR SUBMISSION OF QUESTIONS: Thursday, July 20, 2023 @ 5:00 p.m.

All questions and inquiries shall be formally submitted on this document. Questions shall be submitted in writing and shall reference, whenever possible, the Page, Section, Item number within the Statement of Needs specifications of this document that the question is in reference to.

Answers to all questions received will be issued through a written addendum (if applicable) and become a part of the permanent record of this solicitation.

Project Location: James Madison University
Project # & Title: FDC-1175 Information Technology Consulting Services

RFP Document: Section (number) _____, Page _____, Paragraph _____,

[illegible]

Name	Organization	E-mail Address
------	--------------	----------------

REQUEST FOR PROPOSAL
RFP# FDC-1175

Issue Date: June 15, 2023
Title: Information Technology Consulting 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 August 3, 2023 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 by July 20, 2023 by 5:00 PM E.S.T.

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.

Rev. 3/8/23

REQUEST FOR PROPOSAL

RFP # FDC-1175

TABLE OF CONTENTS

I.	PURPOSE	Page	1
II.	BACKGROUND	Page	1-2
III.	SMALL, WOMAN-OWNED, AND MINORITY PARTICIPATION	Page	2
IV.	STATEMENT OF NEEDS	Page	2-3
V.	PROPOSAL PREPARATION AND SUBMISSION	Page	4-6
VI.	EVALUATION AND AWARD CRITERIA	Page	6-7
VII.	GENERAL TERMS AND CONDITIONS	Page	7-14
VIII.	SPECIAL TERMS AND CONDITIONS	Page	14-18
IX.	METHOD OF PAYMENT	Page	19
X.	PRICING SCHEDULE	Page	19
XI.	ATTACHMENTS	Page	19
	A. Offeror Data Sheet		
	B. SWaM Utilization Plan		
	C. Sample of Standard Contract		
	D. Pricing Schedule		

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit scaled proposals from qualified sources to enter into a contract to provide information technology consulting 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 is a comprehensive university in Harrisonburg, Virginia and is part of the statewide system of public higher education in the Commonwealth. The university offers programs at the bachelor's, master's and doctoral levels with its primary emphasis on the undergraduate student. JMU's current enrollment is approximately 22,000 full and part-time students. The university employs approximately 4,000 faculty and staff. Further information about the University can be found at the following website: www.jmu.edu.

James Madison University's Office of Information Technology is responsible for technology initiatives for campus. JMU was an early adopter of PeopleSoft/Oracle's Campus Solutions product, serving as a beta for its development and implementation. Additionally, the University uses Oracle's PeopleSoft Financials, Human Resources, and the Interaction Hub for JMU's self-service portal. The University also currently uses Oracle's Identity Management suite. JMU actively manages Windows and Macintosh computer systems. The University's network is powered by Cisco technologies. A series of NEC Private Branch Enterprises (PBX's) and gateways constitute the Voice network.

James Madison University is currently utilizing the following technologies:

- Oracle Identity Management Suite 11g R2 P3
- Oracle/PeopleSoft Campus Solutions 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Human Resources 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Financial Management 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Enterprise Application Portal 9.2; PeopleTools 8.55.x
- WebLogic
- Desktop Management: Microsoft Windows and Macintosh (SCCM, JAMF, Apple Enterprise Connect)
- Microsoft 365 (A5 license)
- Microsoft Active Directory
- Federation Services (Shibboleth, OpenID)
- Cisco technologies (including but not limited to network and video conferencing)
- Virtualization technologies (VMWare)
- Cherwell ITSM
- Salesforce (Enterprise CRM)
- NEC Voice and Collaboration Technologies
- Boomi

Additionally, JMU is engaged in a multi-year initiative ("Reengineering Madison") that will include implementing significant technology platforms such as an enterprise Customer Relationship Management (CRM) platform (Salesforce) and new data solutions for managing and visualizing JMU's data. Reengineering Madison will also involve replacing JMU's current PeopleSoft ERP (Enterprise Resource Management) platform, including Finance, Human Resources, and Student Administration applications, as well as current applications used for

managing the identities of JMU's constituents. For more information on Reengineering Madison, see <https://www.jmu.edu/computing/projects/reengineering-madison/index.shtml>.

The University is aware of other cooperative contracts awarded by higher education institutions in the Commonwealth. Firms currently on a cooperative contract with these institutions are not required to respond to this solicitation. The University reserves the right to request quotes from firms on other cooperative contracts, when it is deemed in the best interest of the University.

James Madison University reserves the right, when not in the best interest of the university, to decline award to any firm already on an existing VASCUPP cooperative contract in order to avoid duplication of contracts.

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

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.

1. Describe your corporate competencies/experience providing IT consulting services for one or more of the technologies listed below.
 - a. Oracle Core Technologies
 - b. Oracle/PeopleSoft Enterprise Solutions
 - c. Desktop and Mobile Device Management
 - d. Microsoft Azure and M365
 - e. Okta
 - f. Data Analytics/Visualization/Warehouse/Lake
 - g. Change Management Training, Services, & Certification
 - h. Security and Federation Services
 - i. Cisco Technologies, Infrastructure Support, and Virtualization
 - j. Audio Visual Technologies

- k. Secure Research Enclaves
 - l. Other Technology
2. Describe approach and methodology that will be used to provide IT consulting services to James Madison University. Include how your firm would manage the scope of projects.
 3. Provide the names, qualifications, and experience of personnel to be assigned to James Madison University. Designate who would be assigned as the primary contact for the account.
 4. Describe the ability to provide continuity of consultants throughout the duration of a project.
 5. Describe IT consulting services available from your firm. Examples of services may include, but are not limited to, the following:
 - a. Implementation
 - b. Development
 - c. Project Management
 - d. Architecture and Design
 - e. Capacity Planning
 - f. Installation and Configuration
 - g. Performance and Scalability
 - h. Conversion
 - i. Monitoring, Administration and Upgrades
 - j. Training Development
 - k. Operations Metrics
 6. Describe training options and specify associated costs in *Section X. Pricing Schedule*. Include a catalog of training offerings and differentiation between technical staff and end-user training.
 7. Provide examples of recent projects at higher education institutions comparable to James Madison University. Describe the project, time frame, end result, etc.
 8. Describe the ability to provide for a thorough transfer of knowledge to JMU IT on any given project.
 9. Describe your approach to project management.
 10. Describe how your firm would propose a functional staffing plan indicating the number, characteristics, and schedule for the consultants.
 11. Describe the functions that may be provided by a subcontractor of your firm. Specify the expertise and credentials required from the subcontractor.

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 (*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 from 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 any 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’s 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:

1. Quality of products/services offered and suitability for intended purposes
2. Qualifications and experience of Offeror in providing the goods/services
3. Specific plans or methodology to be used to perform the services
4. Participation of Small, Women-Owned, & Minority (SWaM) Businesses
5. Cost

Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time.

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 I, 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, sexual orientation, gender identity, 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, sexual orientation, gender identity, 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. PRECEDENCE 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, sexual orientation, gender identity, 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.

- Y. CIVILITY IN STATE WORKPLACES: The contractor shall take all reasonable steps to ensure that no individual, while performing work on behalf of the contractor or any subcontractor in connection with this agreement (each, a "Contract Worker"), shall engage in 1) harassment (including sexual harassment), bullying, cyber-bullying, or threatening or violent conduct, or 2) discriminatory behavior on the basis of race, sex, color, national origin, religious belief,

sexual orientation, gender identity or expression, age, political affiliation, veteran status, or disability.

The contractor shall provide each Contract Worker with a copy of this Section and will require Contract Workers to participate in training on civility in the State workplace. Upon request, the contractor shall provide documentation that each Contract Worker has received such training.

For purposes of this Section, "State workplace" includes any location, permanent or temporary, where a Commonwealth employee performs any work-related duty or is representing his or her agency, as well as surrounding perimeters, parking lots, outside meeting locations, and means of travel to and from these locations. Communications are deemed to occur in a State workplace if the Contract Worker reasonably should know that the phone number, email, or other method of communication is associated with a State workplace or is associated with a person who is a State employee.

The Commonwealth of Virginia may require, at its sole discretion, the removal and replacement of any Contract Worker who the Commonwealth reasonably believes to have violated this Section.

This Section creates obligations solely on the part of the contractor. Employees or other third parties may benefit incidentally from this Section and from training materials or other communications distributed on this topic, but the Parties to this agreement intend this Section to be enforceable solely by the Commonwealth and not by employees or other third parties.

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. 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.
- L. 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.
- M. 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.

- N. 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.
- O. 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.
- P. 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.
- 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. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The Contractor assures that information and data obtained as to personal facts and circumstances related to students, faculty, and staff 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*. 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 based on 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 request that our vendors and suppliers enroll in our bank's Comprehensive Payable options: either the Virtual Payables Virtual Card or the PayMode-X electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the Virtual Payables process will receive the benefit of being paid Net 15. 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 onsite and offsite hourly rates broken down by position type for the proposed services. Onsite hourly rates shall include all billables (e.g. travel, lodging, meals, etc.). See Attachment D.

In addition to completing Attachment D, the Offeror shall also provide pricing for all other services, including training offerings.

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: Pricing Schedule

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 SWaM's 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: _____
(Signature)

By: _____
(Signature)

(Printed Name)

(Printed Name)

Title: _____

Title: _____

Attachment D – Pricing Schedule

For each technology/category listed below, provide your company's hourly rate for each of the three roles listed. If you refer to the role by a different name, list it in the space provided next to the corresponding role. Onsite pricing must be inclusive of all billables (travel, lodging, meals, etc.)

***** ***The Offeror shall also provide onsite and offsite pricing for all other services/roles not listed below, including training offerings.*** *****

	Onsite	Offsite		Onsite	Offsite
Oracle Core Technologies			Change Management Training, Svcs, & Cert.		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Oracle/PeopleSoft Enterprise Solutions			Security and Federation Services		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Desktop and Mobile Device Management			Cisco Technologies, Infrastructure Support, and Virtualization		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Microsoft Azure and M365			Audio Visual Technologies		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Okta			Secure Research Enclaves		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Data Analytics/Visualization/Warehouse/Lake			Other Technology		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.

Reference: Addendum 1



July 25, 2023

ADDENDUM NO.: One

TO ALL OFFERORS:

REFERENCE: Request for Proposal No: **RFP# FDC-1175**
Dated: **June 15, 2023**
Commodity: **Information Technology Consulting Services**
RFP Closing On: ~~Thursday, August 3, 2023, at 2:00 p.m.~~
Tuesday, August 15, 2023, at 2:00 p.m.

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

James Madison University has extended the RFP closing date to Tuesday, August 15, 2023 at 2:00 p.m.

Due to the volume of questions received, an additional addendum may be posted at a future date.

1. Question – On the 3rd page of the solicitation it states the period of performance is from date of award through one year (renewable). How many renewals periods does JMU expect in terms of being renewable?
Answer – Section VII. Special Terms and Conditions, Item F states that JMU has the option to extend the original contract for four (4) successive one-year periods.
2. Question – How many FTEs are estimated to be needed onsite versus remote?
Answer – This would depend on the nature of the engagement.
3. Question – In order to be awarded this project, does at least one (1) team member need to be SWaM certified? Do sub-contractors need to be small business and SWaM certified?
Answer – SWaM certification is not a requirement for award; however, JMU tries to work with SWaM vendors whenever possible. Evaluation points will be given to vendors that are a SWaM vendor or that use SWaM sub-contractors. Additionally, all vendors should complete the SWaM Utilization Plan in the RFP document.
4. Question - Is there a page limit to RFP response?
Answer – No; however, proposals should be prepared simply and economically (see section V.A.3.b.).
5. Question – What industry partner currently performs this work? What is the incumbent contract number and total dollar value if there is one? Please confirm if we can get the previous proposals or pricing of the incumbent(s).
Answer – The University currently has contracts in place with the following vendors - Unicon, Inc., Sierra-Cedar, Inc., Securance Consulting, HyperGen, Inc, Plante & Moran, PLLC, Cherry Bekaert Advisory

MSC 5720
752 Ott Street, Room 1042
Wine Price Building
Harrisonburg, VA 22807
Office of 540.568.3145 Phone
PROCUREMENT SERVICES 540.568.7935 Fax

LLC, Highstreet IT Solutions, LLC, Nautiquos Business Solutions, LLC, Assura, Inc., and Planet Technologies, Inc. Previous spend can be found at www.eva.virginia.gov. Current contracts with the firms listed above can be found at <http://cipag.jmu.edu/cipag/>.

6. Question - Is remote only pricing an option? Will proposals be considered if only remote pricing is provided?
Answer – All proposals will be considered, including remote only pricing.
7. Question – Can vendors only provide pricing for select areas as opposed to all areas?
Answer – Offerors may provide pricing for one or more of the technologies/categories listed in the RFP (see *Section IV.I*). Offerors should identify their firm’s technology specializations in their proposal.
8. Question – Is hosting included as part of the services required?
Answer – The scope may include hosting services, depending on the specific project.
9. Question – Is operations and maintenance – patching, vulnerability scanning, remediation, etc. included as a part of the services requested?
Answer – The scope may include operations and maintenance services, depending on the specific project.
10. Question – Given that Oracle’s Identity Management is currently used at JMU, how does JMU anticipate using Okta?
Answer – The University has selected Okta as its future Identity Management solution.
11. Question – What is meant by Secure Research Enclaves?
Answer - Using Microsoft’s definition, the Secure Enclave for Research (also known as the Secure Research Enclave) is a reference architecture for a remotely-accessible environment for researchers to use in a secure manner while working on restricted data sets.
12. Question – Does the scope of the contract include the design and implementation of any hybrid cloud infrastructure?
Answer – The scope may include the design and implementation of cloud/hybrid cloud infrastructure, depending on the specific project.
13. Question – What criteria does the University use to accept or reject proposed or assigned consultants, and how does this impact the contractor’s role and responsibilities throughout the duration of the contract?
Answer – Consultants assigned to the University may be rejected based on a variety of reasons including, but not limited to, lack in professionalism, responsiveness, timeliness, knowledge and experience, etc.
14. Question – Is the work expected to be SOW based or hourly based?
Answer – That will depend on the nature of the engagement; however, it is reasonable to expect that either could apply.
15. Question – It is mentioned that sealed proposals will be received. Is there any that a vendor can submit a proposal online?
Answer – No. JMU is not set up to receive electronic responses through eVA or emailed proposal responses.

16. Question – What is the annual spend at JMU for IT consulting services?
Answer – Previous spend can be found at www.eva.virginia.gov.
17. Question – Assuming an offeror currently holds a contract with a VASCUPP higher education institution, such as the University of Virginia or George Mason University, how does that impact our status on this RFP?
Answer – The last paragraph of the *Section II. Background* section states: “James Madison University reserves the right, when not in the best interest of the university, to decline award to any firm already on an existing VASCUPP cooperative contract in order to avoid duplication of contracts.”
18. Question – Will you prefer vendors with a branch office presence in Harrisonburg? We are only present in Northern Virginia.
Answer – A branch office in Harrisonburg, VA is not required.
19. Question - Are there specific technologies within the listed categories (such as Oracle Core Technologies, Microsoft Azure, etc.) that require specialized expertise or are of higher priority in the context of JMU's Reengineering Madison?
Answer – See RFP *Section II. Background*.
20. Question - Can you provide more information about the typical scope and size of projects at James Madison University? Are there any specific project management methodologies or frameworks that the university prefers? Do you have any major projects in progress?
Answer – The University's major technology projects can be found at <https://www.jmu.edu/computing/projects-and-initiatives.shtml>.
21. Question - What is the expected duration of the projects? Will the assignments be short-term or long-term?
Answer – The expected duration will depend on the specific project and may be short-term or long-term.
22. Question - Are there any specific certifications or qualifications required for the assigned personnel?
Answer – Required certifications or qualifications will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP *Section IV.3*).
23. Question - Can you provide more details on the expected level of involvement and responsibilities of the primary contact for the account?
Answer – Expected level of involvement and responsibilities will vary based on the project.
24. Question - Can you provide more information about the evaluation criteria for assessing the similarity of projects at higher education institutions?
Answer – Offerors should provide examples of recent projects at higher education institutions comparable to James Madison University. See RFP *Section II. Background* for more information about the University.
25. Question - Are there any specific reporting or documentation requirements for IT consulting services?
Answer – Reporting and documentation requirements will vary depending on the project.
26. Question – Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time. When will this be posted?
Answer – The points will be posted the day before the RFP closes.

27. Question - Does the scope include advising and strategic planning support for the technologies listed?
Answer – The scope may include advising and strategic planning support, depending on the specific project.
28. Question - What will be the engagement model for Vendors that are awarded this contract? Will JMU issue statements of work for the selected vendors to compete? Will the statements of work be for hourly staff augmentation or will it also include fixed price strategic engagements? Can you provide additional information on the anticipated level of collaboration and coordination between the successful bidder and JMU IT staff?
Answer – As information technology consulting needs arise, the University will contact a firm(s) on contract to discuss the project for which the University requires assistance. A statement of work will be requested from the vendor based on contract terms and pricing, and additional discussions will occur.
29. Question - What will be the maximum number of awardees under this contract? Please confirm the anticipated number of awards.
Answer – The University does not have an anticipated or maximum number of awards for this RFP.
30. Question – For this RFP, are resources expected to be on-site or remote in Harrisonburg, VA? Given the skill sets, we're assuming it's fully remote, but wanted to verify
Answer – Remote is usually acceptable; however, it would depend on the nature of the engagement.
31. Question - How many users are on Office 365? What license do they have? Provide a license count.
Answer – Approximately 30,000 accounts. The majority have A5 licenses with a few having A3 licenses.
32. Question - Are the licenses being purchased directly with Microsoft or through a Microsoft Partner?
Answer – SHI.
33. Question - Do you currently use Microsoft Teams and/or Microsoft SharePoint?
Answer – Yes.
34. Question - Is there a software in place currently to manage endpoints remotely? If so, what product(s) are being used?
Answer - JAMF Pro, Microsoft Intune, and Microsoft Endpoint Configuration Manager are used.
35. Question - How often are the devices and endpoints being updated? Monthly/quarterly/etc. basis?
Answer – Endpoint patches are deployed typically the same month they become available.
36. Question - Do you have employees working remotely that use a company device?
Answer – Yes.
37. Question - Do you offer Bring Your Own Device (BYOD) to employees?
Answer – No.
38. Question - Is there a Mobile Device Management (MDM) solution deployed?
Answer – Yes, for JMU owned devices.

39. Question - How many desktops/laptops/mobile devices are you supporting?
Answer – JMU IT actively manages roughly 4,500 Windows devices, 2,500 Mac devices, and 1,000 mobile devices.
40. Question - Which version of Windows are the desktops/laptops running on?
Answer – Primarily Windows 10 22H2.
41. Question - Are user devices being backed up? If so, how often, and do you have retention policies in place?
Answer – User devices are not centrally backed up.
42. Question – Are the servers on-site or on the cloud? Hybrid?
Answer - Servers are onsite.
43. If you have a cloud environment, is it Azure/AWS/other?
Answer – The University has applications in both Azure and AWS.
44. Question - How many servers do you have? What operating system are they on? Do you have any Windows Server 2012/2012R2? Any Linux Servers? Microsoft is sunsetting Windows 2012 servers in October. Is there a plan to upgrade/replace your current 2012 servers? Please provide details.
Answer – The University has approximately 500 servers. Windows and Linux.
- 2012R2 (26 servers - all slated to decom by October, with the potential exception of 3 belonging to Card Services, which they handle on their own and are in discussions with IT-Sec about)
 - 2016 (89 servers)
 - 2019 (93 servers)
 - 2022 (7 servers)
 - Linux (210 Servers) primarily running RHEL 7 & 8
 - 16 - VMware Host servers, and 3 management servers, running VMWare version 7. (13 normal hosts, 3 VDI hosts, 2 VCenter servers and the VRealize server)
 - 54 - additional servers are being tracked, but are either security servers (OS not maintained by us), Other Linux (CentOS) or OVAs (Virtual appliances)
45. Question - Is there a Disaster Recovery plan in place? What is the infrastructure at the fail over location?
Answer - Yes. Disaster Recovery plans exist for critical systems. There is geographical, power, and HVAC redundancy at the failover location, as well as off-site backups in the event of whole data center loss.
46. Question - How many databases are you using? Please specify which ones.
Answer – See RFP *Section II. Background*.
47. Question - What are some of the critical applications being used today? Any ERP applications?
Answer – See RFP *Section II. Background*.
48. Question - What is the network topology currently used, and how are these locations communicating to each other?
Answer - On campus locations are serviced via single mode fiber. Off campus locations are a combination of DIA circuits and wireless bridges.

49. Question - Is there a VPN in place for remote access? Is there a firewall?
Answer - Yes to both.
50. Question - What is the speed of the network connection to the internet? Do you have a backup connection?
Answer - Two 8Gbs pipes in active/active state.
51. Question - How many Routers, Switches, and Firewalls are in your network?
Answer - L2 switches: 855
L3 switches/routers: 10
Firewalls: 4
52. Question - How many buildings/locations?
Answer – The University has approximately 185 buildings on 750 acres. The campus is divided by interstate 81 and the C&P railroad.
53. Question - How big is your current IT department, if any?
Answer - Approximately 150 employees
54. Question - Please provide the brand for the switches, network devices, laptops, desktops, and printers.
Answer - Cisco Routers and switches for the wired network. The wireless network is Aruba.
Laptop/Desktops are a mix of Dell and Apple. Printers vary, but a significant number are leased KM Bizhub devices.
55. Question - Do you have any cameras to support?
Answer: Yes. Cameras are managed by Facilities Management.
56. Question - Do you currently have a VOIP solution? Who is your VOIP provider? What is the brand of your desktop phones? How many extensions/DID numbers?
Answer – The University is currently deploying an NEC VoIP solution with Black Box Network Services, and have approximately 8,000 user and service type extensions. Phones are NEC.
57. Question - Do you have ticketing system in place? Estimate of tickets per month/quarter?
Answer - Yes. The University uses Cherwell as its ITSM ticketing system and receives approximately 49,189 tickets per year.
58. Question - Do you require someone to be on-site all the time?
Answer - That would depend on the nature of the engagement.
59. Question - Is this a multi-vendor or single vendor award?
Answer – This is anticipated to be a multi-award contract.
60. Question - Is there Change Management system in place?
Answer - Technical hardware or software changes are managed through the University's ITSM.
61. Question - Is there an Information Technology Asset Management (ITAM) solution in place?
Answer – Not as such. The University uses Cherwell ITSM for CMDB, and JAMF Pro and Intune for MDM.

62. Question - What applications are currently in use?

Answer – See RFP *Section II. Background.*

63. Question - The RFP has some focus on Salesforce in the opening. But I see that Huron was awarded a contract for Salesforce work less than 6 months ago. Is JMU looking to understand other options that can support the Salesforce deployment if needed?

Answer – Yes, the University is interested in other Salesforce resources and skillset augmentation options.

64. Question – Are there any pain points of issues with the current vendor(s)?

Answer – No.

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

Reference: Addendum 2



August 3, 2023

ADDENDUM NO.: Two

TO ALL OFFERORS:

REFERENCE: Request for Proposal No: **RFP# FDC-1175**
Dated: **June 15, 2023**
Commodity: **Information Technology Consulting Services**
RFP Closing On: **Tuesday, August 15, 2023, at 2:00 p.m.**

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

1. Question - How far along is the Reengineering Madison project? When is the new system expected to go live?
Answer - See RFP Section II. Background.
2. Question - Can you please share the portfolio of projects/initiatives that will be executed under the Reengineering Madison program?
Answer - See RFP Section II. Background.
3. Question - Can you provide ticket volumes that you are currently experiencing for PeopleSoft for the last one year, preferably by severity?
Answer - No. Ticket volume alone is not a good indicator.
4. Question - What is the size of the existing support team supporting PeopleSoft?
Answer - 10 people.
5. Question - Will existing support team members be moved to the Reengineering Madison project?
Answer - Yes, in part.
6. Question - Can you provide the architecture diagram for your PeopleSoft application and its deployment?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
7. Question - What is the current PUM level for each of the PeopleSoft application pillar?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
8. Question - What is the number of environments that exist for each PeopleSoft application pillar (example – DEV, TEST, DMO, UAT etc.)?
Answer - 4 environments.

MSC 5720
752 Ott Street, Room 1042
Wine Price Building
Harrisonburg, VA 22807
Office of 540.568.3145 Phone
PROCUREMENT SERVICES 540.568.7935 Fax

9. Question - What is the size of the production database for each of the PeopleSoft application pillar?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
10. Question - Does Oracle Core Technologies mean the Oracle DBA skill set? If not, please provide more details.
Answer - Yes.
11. Question - What skills are required in Desktop and Mobile Device Management?
Answer - Required skills, certifications, or qualifications will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP *Section IV.3.*).
12. Question - Please provide details of the services expected in the following technologies:
a. Security and Federation Services
b. Microsoft 365 (M365)
c. Audio and Visual Technologies
d. Secure Research Enclaves
Answer - Services may vary depending on the nature of the engagement.
13. Question - What is expected from Svcs and Cert in Change Management? What are the roles of Senior Engineer/Engineer in Change Management?
Answer - See RFP *Section IV. Statement of Needs and Section D. Pricing Schedule.* If your firm refers to a specific role by a different name, list it in the space provided next to the corresponding role.
14. Question - Does onsite pricing refer to work specifically performed on campus (in person), and does offsite work pertain to work conducted within the US but off-campus, remote?
Answer - Yes.
15. Question - What positions are you looking to fill immediately? Is there current or future project you are expecting?
Answer - See RFP *Section II. Background.*
16. Question - For onsite services, we find that a base billable rate is suitable for most of our clients, and hotel/travel expenses charged as actuals later. Would you still like a single blended hourly charge for these positions including all expenses?
Answer - Yes.
17. Question - What are the Oracle core technologies focused on consulting services like OBIA, OBIEE, ODI, OAC, etc.?
Answer – Unavailable at this time.
18. Question - Is there a preferred cloud provider like AWS, GCP, or Azure for a data lake/data warehouse solution?
Answer - No.
19. Question - Is the data warehouse/data lake solution in place that required migrating to a new tool stack or a new solution is expected?
Answer - See RFP *Section II. Background.*

20. Question - Is there a preferred visualization tool for analytics?
Answer - No.
21. Question - Has Fluid UI been implemented in your PeopleSoft Application?
Answer - No.
22. Question - Is the Boomi atom/molecule installed on-premises or in the cloud?
Answer – On-premises.
23. Question - What Salesforce modules have been implemented/utilized?
Answer - Implementation is just beginning. See RFP *Section II. Background*.
24. Question - Is it mandatory to showcase the amount of sales our company had during the last twelve months with each VASCUPP Member Institution? Can we skip this portion if we do not have an existing/ previous VASCUPP cooperative contract? Will the proposal be deemed non-responsive if we do not have sales during the last twelve months with each VASCUPP Member Institution?
Answer - A response to the question is required. If the answer is none/zero, indicate that as your answer. Previous sales/experience with a VASCUPP Member Institution is not a requirement for submitting a proposal or being awarded a contract.
25. Question - Please confirm whether the "Secure Research Enclave" category includes CMMC readiness testing? Or, is this category meant for the development/implementation of the architecture for these enclaves?
Answer - Secure Research Enclave could include CMMC readiness or the development/implementation of the architecture for these enclaves.
26. Question - How does JMU define "Consulting Services" and "technology advisor"?
Answer - See RFP *Section IV. Statement of Needs*.
27. Question - Is this a new requirement or an existing requirement?
Answer - This RFP is to replace an existing contract with multiple vendors.
28. Question - What are your Key Performance Indicators?
Answer - Key performance indicators will vary depending on the project.
29. Question - If we have a teaming agreement with a subcontractor, does the subcontractor's experience count as experience for us?
Answer - The experience of a subcontractor specified in a proposal may be considered in the evaluation of the qualifications and experience of the Offeror.
30. Question - Do we need to submit only one response including the price schedule?
Answer - Vendors should submit one (1) original and four (4) copies, and electronic copy in WORD format or searchable PDF (*on a flash drive*) of the entire proposal, INCLUDING ALL ATTACHMENTS. The original, copies, and electronic version should all be the same and include the pricing schedule.

31. Question - As a firm registered on eVA, do we have to pay the fees before the submission of the proposal (i.e. this stage) or after award? Please also clarify that the subcontractor also has to pay this fee.

Answer - eVA fees are only paid upon receipt of a purchase order issued through the eVA system. eVA fees are paid by the vendor listed on the issued purchase order. If a subcontractor is issued a purchase order directly, they would have to pay the associated eVA fees; however, if the purchase order is issued to the prime contractor, and the subcontractor is working under the prime contractor, the subcontractor would not pay the associated eVA fees. The University typically issues purchase orders to the prime contractor.

32. Question - Do we need to submit provided RFP Cover Sheet as a Cover Page of the proposal?

Answer - The RFP cover sheet does not need to be submitted as the cover page of a proposal.

33. Question - Is there any local preference for this contract?

Answer - No.

34. Question - Is it mandatory to have experience with higher education institutions?

Answer - Experience with higher education institutions is not required.

35. Question - Please confirm whether security assessment and consulting services are included on this contract. If so, should we price this under the category "Security and Federation Services" on the Pricing Schedule?

Answer - The scope may include security assessment and consulting services, depending on the specific project. In addition to completing *Attachment D*, Offerors should also provide pricing for all other services.

36. Question - Is there any flexibility in the initial contract duration of one year? Is it safe to assume that the same terms and conditions will remain same when the project is renewed? Are there any pre-defined criteria to be met by the vendors to get the renewal of contract?

Answer - JMU typically issues contracts for one year with subsequent one-year renewals. The terms and conditions of existing term contracts are reviewed at the time of renewal. Contract terms may be negotiated and modified as necessary. See RFP *Section VIII.F*.

37. Question - Can you please specify the list of all technologies in each technology area under Section IV? Example: Do we need to consider Oracle Database, Fusion Middleware, SOA, BPM, Identity Management, MDM, Webcenter-Sites, Portal, Content, Social, OBIEE, Golden Gate and ODI when you refer to Oracle Core Technologies? Similarly, can you call out all technologies under each area?

Answer – See RFP *Section II. Background*.

38. Question - Can you provide more information about the technologies listed in Section II of the RFP, such as Oracle Core Technologies, PeopleSoft Enterprise Solutions, Microsoft Azure, Okta, etc.? What level of expertise and experience is JMU looking for in these areas?

Answer – The level of expertise and experience required will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP *Section IV.3*).

39. Question - What are the expected outcomes of the trainings that a vendor needs to provide to the staff? How much training must be provided in a month? What will be the number of attendees in each session? Will it be a virtual or classroom training?
Answer – Training outcomes, frequency, number of attendees, format, etc. will vary depending on specific training needs and agreed upon SOW.
40. Question - Can you provide more details about the weightage or scoring system that will be used to evaluate proposals based on the criteria stated in the RFP? How will the award decision be made?
Answer - See RFP *Section IV. Evaluation and Award Criteria*. Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time.
41. Question - Can you provide more information on the Virtual Payables options mentioned? How can vendors and suppliers enroll in these options?
Answer - Offerors may contact the JMU Accounts Payable office, at acctspayable@jmu.edu or (540) 568-7397 to discuss payment enrollment options.
42. Question - Please list all the technologies/tools that needs to be replaced/transformed as part of Reengineering Madison program. Are there specific projects the vendor team will be involved if selected?
Answer - See RFP *Section II. Background*.
43. Question - Does the University anticipate any of its current implementation partners will act as a Systems/Services Integrator and an offeror submitting a proposal in response to this solicitation act as subcontractor if selected?
Answer - No.
44. Question - Are you engaged with any cloud service provider? What is the scope of cloud-based solutions in this RFP?
Answer - See RFP *Section II. Background*.
45. Question - What are your expectations for the level of service that you would like to receive from the IT consulting firm? How would you measure the success of the IT consulting project?
Answer - Expectations and measurements of success will vary depending on the engagement.
46. Question - What are your expectations for the level of security that you would like to have in place?
Answer - JMU follows the ISO standard. When needed other standards are used depending on the need, regulations, requirements, etc.
47. Question - What are the specific challenges that you are facing with your current IT infrastructure compelling to go through Re-engineering Initiative?
Answer - See RFP *Section II. Background*.
48. Question - Could you provide more information about the anticipated scope of special projects where the contractor will serve as a technology expert? What are some examples of these projects and their objectives? Can you elaborate the expected deliverables and milestones for the projects covered in the scope this RFP?
Answer - See RFP *Section II. Background*.

49. Question - Is there any preference for local or regional vendors?

Answer - No.

50. Question - Is it safe to assume that offsite means offshore?

Answer - No. **For the purpose of this solicitation, offsite means remote work performed not on campus.**

51. Question - Resources working offshore need to align with client working hours as per US time zones?

Answer - Yes.

52. Question - Will JMU provide laptops to the vendor consultants?

Answer - No.

53. Question - Will any additional travel costs be considered in the pricing?

Answer - No. **See RFP Section X. Pricing Schedule.**

Signify receipt of this addendum by initialing "*Addendum #2*_____" on the signature page of your proposal.

Sincerely,

Doug Chester
Buyer Senior
Phone: 540-568-4272



Request for Proposal

RFP# FDC-1175

Information Technology Consulting Services

June 15, 2023



Name	Organization	E-mail Address
------	--------------	----------------

REQUEST FOR PROPOSAL

RFP# FDC-1175

Issue Date: June 15, 2023

Title: Information Technology Consulting 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 August 3, 2023 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 by July 20, 2023 by 5:00 PM EST.

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-1175

TABLE OF CONTENTS

I.	PURPOSE	Page	1
II.	BACKGROUND	Page	1-2
III.	SMALL, WOMAN-OWNED, AND MINORITY PARTICIPATION	Page	2
IV.	STATEMENT OF NEEDS	Page	2-3
V.	PROPOSAL PREPARATION AND SUBMISSION	Page	4-6
VI.	EVALUATION AND AWARD CRITERIA	Page	6-7
VII.	GENERAL TERMS AND CONDITIONS	Page	7-14
VIII.	SPECIAL TERMS AND CONDITIONS	Page	14-18
IX.	METHOD OF PAYMENT	Page	19
X.	PRICING SCHEDULE	Page	19
XI.	ATTACHMENTS	Page	19
	A. Offeror Data Sheet		
	B. SWaM Utilization Plan		
	C. Sample of Standard Contract		
	D. Pricing Schedule		

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 consulting 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 is a comprehensive university in Harrisonburg, Virginia and is part of the statewide system of public higher education in the Commonwealth. The university offers programs at the bachelor's, master's and doctoral levels with its primary emphasis on the undergraduate student. JMU's current enrollment is approximately 22,000 full and part-time students. The university employs approximately 4,000 faculty and staff. Further information about the University can be found at the following website: www.jmu.edu.

James Madison University's Office of Information Technology is responsible for technology initiatives for campus. JMU was an early adopter of PeopleSoft/Oracle's Campus Solutions product, serving as a beta for its development and implementation. Additionally, the University uses Oracle's PeopleSoft Financials, Human Resources, and the Interaction Hub for JMU's self-service portal. The University also currently uses Oracle's Identity Management suite. JMU actively manages Windows and Macintosh computer systems. The University's network is powered by Cisco technologies. A series of NEC Private Branch Enterprises (PBX's) and gateways constitute the Voice network.

James Madison University is currently utilizing the following technologies:

- Oracle Identity Management Suite 11g R2 P3
- Oracle/PeopleSoft Campus Solutions 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Human Resources 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Financial Management 9.2; PeopleTools 8.55.x
- Oracle/PeopleSoft Enterprise Application Portal 9.2; PeopleTools 8.55.x
- WebLogic
- Desktop Management: Microsoft Windows and Macintosh (SCCM, JAMF, Apple Enterprise Connect)
- Microsoft 365 (A5 license)
- Microsoft Active Directory
- Federation Services (Shibboleth, OpenID)
- Cisco technologies (including but not limited to network and video conferencing)
- Virtualization technologies (VMWare)
- Cherwell ITSM
- Salesforce (Enterprise CRM)
- NEC Voice and Collaboration Technologies
- Boomi

Additionally, JMU is engaged in a multi-year initiative ("Reengineering Madison") that will include implementing significant technology platforms such as an enterprise Customer Relationship Management (CRM) platform (Salesforce) and new data solutions for managing and visualizing JMU's data. Reengineering Madison will also involve replacing JMU's current PeopleSoft ERP (Enterprise Resource Management) platform, including Finance, Human Resources, and Student Administration applications, as well as current applications used for

managing the identities of JMU's constituents. For more information on Reengineering Madison, see <https://www.jmu.edu/computing/projects/reengineering-madison/index.shtml>.

The University is aware of other cooperative contracts awarded by higher education institutions in the Commonwealth. Firms currently on a cooperative contract with these institutions are not required to respond to this solicitation. The University reserves the right to request quotes from firms on other cooperative contracts, when it is deemed in the best interest of the University.

James Madison University reserves the right, when not in the best interest of the university, to decline award to any firm already on an existing VASCUPP cooperative contract in order to avoid duplication of contracts.

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

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.

1. Describe your corporate competencies/experience providing IT consulting services for one or more of the technologies listed below.
 - a. Oracle Core Technologies
 - b. Oracle/PeopleSoft Enterprise Solutions
 - c. Desktop and Mobile Device Management
 - d. Microsoft Azure and M365
 - e. Okta
 - f. Data Analytics/Visualization/Warehouse/Lake
 - g. Change Management Training, Services, & Certification
 - h. Security and Federation Services
 - i. Cisco Technologies, Infrastructure Support, and Virtualization
 - j. Audio Visual Technologies

- k. Secure Research Enclaves
 - l. Other Technology
- 2. Describe approach and methodology that will be used to provide IT consulting services to James Madison University. Include how your firm would manage the scope of projects.
- 3. Provide the names, qualifications, and experience of personnel to be assigned to James Madison University. Designate who would be assigned as the primary contact for the account.
- 4. Describe the ability to provide continuity of consultants throughout the duration of a project.
- 5. Describe IT consulting services available from your firm. Examples of services may include, but are not limited to, the following:
 - a. Implementation
 - b. Development
 - c. Project Management
 - d. Architecture and Design
 - e. Capacity Planning
 - f. Installation and Configuration
 - g. Performance and Scalability
 - h. Conversion
 - i. Monitoring, Administration and Upgrades
 - j. Training Development
 - k. Operations Metrics
- 6. Describe training options and specify associated costs in *Section X. Pricing Schedule*. Include a catalog of training offerings and differentiation between technical staff and end-user training.
- 7. Provide examples of recent projects at higher education institutions comparable to James Madison University. Describe the project, time frame, end result, etc.
- 8. Describe the ability to provide for a thorough transfer of knowledge to JMU IT on any given project.
- 9. Describe your approach to project management.
- 10. Describe how your firm would propose a functional staffing plan indicating the number, characteristics, and schedule for the consultants.
- 11. Describe the functions that may be provided by a subcontractor of your firm. Specify the expertise and credentials required from the subcontractor.

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** (*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 from 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 any 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’s 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:

1. Quality of products/services offered and suitability for intended purposes
2. Qualifications and experience of Offeror in providing the goods/services
3. Specific plans or methodology to be used to perform the services
4. Participation of Small, Women-Owned, & Minority (SWaM) Businesses
5. Cost

Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time.

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, sexual orientation, gender identity, 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, sexual orientation, gender identity, 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. PRECEDENCE 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, sexual orientation, gender identity, 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.
- Y. CIVILITY IN STATE WORKPLACES: The contractor shall take all reasonable steps to ensure that no individual, while performing work on behalf of the contractor or any subcontractor in connection with this agreement (each, a "Contract Worker"), shall engage in 1) harassment (including sexual harassment), bullying, cyber-bullying, or threatening or violent conduct, or 2) discriminatory behavior on the basis of race, sex, color, national origin, religious belief,

sexual orientation, gender identity or expression, age, political affiliation, veteran status, or disability.

The contractor shall provide each Contract Worker with a copy of this Section and will require Contract Workers to participate in training on civility in the State workplace. Upon request, the contractor shall provide documentation that each Contract Worker has received such training.

For purposes of this Section, "State workplace" includes any location, permanent or temporary, where a Commonwealth employee performs any work-related duty or is representing his or her agency, as well as surrounding perimeters, parking lots, outside meeting locations, and means of travel to and from these locations. Communications are deemed to occur in a State workplace if the Contract Worker reasonably should know that the phone number, email, or other method of communication is associated with a State workplace or is associated with a person who is a State employee.

The Commonwealth of Virginia may require, at its sole discretion, the removal and replacement of any Contract Worker who the Commonwealth reasonably believes to have violated this Section.

This Section creates obligations solely on the part of the contractor. Employees or other third parties may benefit incidentally from this Section and from training materials or other communications distributed on this topic, but the Parties to this agreement intend this Section to be enforceable solely by the Commonwealth and not by employees or other third parties.

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. 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.
- L. 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.
- M. 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.

- N. 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.
- O. 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.
- P. 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.
- 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. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The Contractor assures that information and data obtained as to personal facts and circumstances related to students, faculty, and staff 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*. 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 based on 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 request that our vendors and suppliers enroll in our bank's Comprehensive Payable options: either the Virtual Payables Virtual Card or the PayMode-X electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the Virtual Payables process will receive the benefit of being paid Net 15. 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 onsite and offsite hourly rates broken down by position type for the proposed services. Onsite hourly rates shall include all billables (e.g. travel, lodging, meals, etc.). See Attachment D.

In addition to completing Attachment D, the Offeror shall also provide pricing for all other services, including training offerings.

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: Pricing Schedule

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: _____
(Signature)

By: _____
(Signature)

(Printed Name)

(Printed Name)

Title: _____

Title: _____

Attachment D – Pricing Schedule

For each technology/category listed below, provide your company's hourly rate for each of the three roles listed. If you refer to the role by a different name, list it in the space provided next to the corresponding role. Onsite pricing must be inclusive of all billables (travel, lodging, meals, etc.)

******* The Offeror shall also provide onsite and offsite pricing for all other services/roles not listed below, including training offerings. *******

	Onsite	Offsite		Onsite	Offsite
Oracle Core Technologies			Change Management Training, Svcs, & Cert.		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Oracle/PeopleSoft Enterprise Solutions			Security and Federation Services		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Desktop and Mobile Device Management			Cisco Technologies, Infrastructure Support, and Virtualization		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Microsoft Azure and M365			Audio Visual Technologies		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Okta			Secure Research Enclaves		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.
Data Analytics/Visualization/Warehouse/Lake			Other Technology		
Project Manager or _____	_____/hr.	_____/hr.	Project Manager or _____	_____/hr.	_____/hr.
Senior Engineer or _____	_____/hr.	_____/hr.	Senior Engineer or _____	_____/hr.	_____/hr.
Engineer or _____	_____/hr.	_____/hr.	Engineer or _____	_____/hr.	_____/hr.



July 25, 2023

ADDENDUM NO.: One

TO ALL OFFERORS:

REFERENCE: Request for Proposal No: **RFP# FDC-1175**
Dated: **June 15, 2023**
Commodity: **Information Technology Consulting Services**
RFP Closing On: ~~Thursday, August 3, 2023, at 2:00 p.m.~~
Tuesday, August 15, 2023, at 2:00 p.m.

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

James Madison University has extended the RFP closing date to Tuesday, August 15, 2023 at 2:00 p.m.

Due to the volume of questions received, an additional addendum may be posted at a future date.

1. Question – On the 3rd page of the solicitation it states the period of performance is from date of award through one year (renewable). How many renewals periods does JMU expect in terms of being renewable?
Answer – Section VII. Special Terms and Conditions, Item F states that JMU has the option to extend the original contract for four (4) successive one-year periods.
2. Question – How many FTEs are estimated to be needed onsite versus remote?
Answer – This would depend on the nature of the engagement.
3. Question – In order to be awarded this project, does at least one (1) team member need to be SWaM certified? Do sub-contractors need to be small business and SWaM certified?
Answer – SWaM certification is not a requirement for award; however, JMU tries to work with SWaM vendors whenever possible. Evaluation points will be given to vendors that are a SWaM vendor or that use SWaM sub-contractors. Additionally, all vendors should complete the SWaM Utilization Plan in the RFP document.
4. Question - Is there a page limit to RFP response?
Answer – No; however, proposals should be prepared simply and economically (see section V.A.3.b.).
5. Question – What industry partner currently performs this work? What is the incumbent contract number and total dollar value if there is one? Please confirm if we can get the previous proposals or pricing of the incumbent(s).
Answer – The University currently has contracts in place with the following vendors - Unicon, Inc., Sierra-Cedar, Inc., Securance Consulting, HyperGen, Inc, Plante & Moran, PLLC, Cherry Bekaert Advisory

MSC 5720
752 Ott Street, Room 1042
Wine Price Building
Harrisonburg, VA 22807
540.568.3145 Phone
540.568.7935 Fax
Office of
PROCUREMENT SERVICES

LLC, Highstreet IT Solutions, LLC, Nautiquos Business Solutions, LLC, Assura, Inc., and Planet Technologies, Inc. Previous spend can be found at www.eva.virginia.gov. Current contracts with the firms listed above can be found at <http://cipag.jmu.edu/cipag/>.

6. Question - Is remote only pricing an option? Will proposals be considered if only remote pricing is provided?
Answer – All proposals will be considered, including remote only pricing.
7. Question – Can vendors only provide pricing for select areas as opposed to all areas?
Answer – Offerors may provide pricing for one or more of the technologies/categories listed in the RFP (see Section IV.1.). Offerors should identify their firm’s technology specializations in their proposal.
8. Question – Is hosting included as part of the services required?
Answer – The scope may include hosting services, depending on the specific project.
9. Question – Is operations and maintenance – patching, vulnerability scanning, remediation, etc. included as a part of the services requested?
Answer – The scope may include operations and maintenance services, depending on the specific project.
10. Question – Given that Oracle’s Identity Management is currently used at JMU, how does JMU anticipate using Okta?
Answer – The University has selected Okta as its future Identity Management solution.
11. Question – What is meant by Secure Research Enclaves?
Answer - Using Microsoft’s definition, the Secure Enclave for Research (also known as the Secure Research Enclave) is a reference architecture for a remotely-accessible environment for researchers to use in a secure manner while working on restricted data sets.
12. Question – Does the scope of the contract include the design and implementation of any hybrid cloud infrastructure?
Answer – The scope may include the design and implementation of cloud/hybrid cloud infrastructure, depending on the specific project.
13. Question – What criteria does the University use to accept or reject proposed or assigned consultants, and how does this impact the contractor’s role and responsibilities throughout the duration of the contract?
Answer – Consultants assigned to the University may be rejected based on a variety of reasons including, but not limited to, lack in professionalism, responsiveness, timeliness, knowledge and experience, etc.
14. Question – Is the work expected to be SOW based or hourly based?
Answer – That will depend on the nature of the engagement; however, it is reasonable to expect that either could apply.
15. Question – It is mentioned that sealed proposals will be received. Is there any that a vendor can submit a proposal online?
Answer – No. JMU is not set up to receive electronic responses through eVA or emailed proposal responses.

16. Question – What is the annual spend at JMU for IT consulting services?
Answer – Previous spend can be found at www.eva.virginia.gov.
17. Question – Assuming an offeror currently holds a contract with a VASCUPP higher education institution, such as the University of Virginia or George Mason University, how does that impact our status on this RFP?
Answer – The last paragraph of the *Section II. Background* section states: “James Madison University reserves the right, when not in the best interest of the university, to decline award to any firm already on an existing VASCUPP cooperative contract in order to avoid duplication of contracts.”
18. Question – Will you prefer vendors with a branch office presence in Harrisonburg? We are only present in Northern Virginia.
Answer – A branch office in Harrisonburg, VA is not required.
19. Question - Are there specific technologies within the listed categories (such as Oracle Core Technologies, Microsoft Azure, etc.) that require specialized expertise or are of higher priority in the context of JMU’s Reengineering Madison?
Answer – See RFP *Section II. Background*.
20. Question - Can you provide more information about the typical scope and size of projects at James Madison University? Are there any specific project management methodologies or frameworks that the university prefers? Do you have any major projects in progress?
Answer – The University’s major technology projects can be found at <https://www.jmu.edu/computing/projects-and-initiatives.shtml>.
21. Question - What is the expected duration of the projects? Will the assignments be short-term or long-term?
Answer – The expected duration will depend on the specific project and may be short-term or long-term.
22. Question - Are there any specific certifications or qualifications required for the assigned personnel?
Answer – Required certifications or qualifications will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP *Section IV.3*).
23. Question - Can you provide more details on the expected level of involvement and responsibilities of the primary contact for the account?
Answer – Expected level of involvement and responsibilities will vary based on the project.
24. Question - Can you provide more information about the evaluation criteria for assessing the similarity of projects at higher education institutions?
Answer – Offerors should provide examples of recent projects at higher education institutions comparable to James Madison University. See RFP *Section II. Background* for more information about the University.
25. Question - Are there any specific reporting or documentation requirements for IT consulting services?
Answer – Reporting and documentation requirements will vary depending on the project.
26. Question – Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time. When will this be posted?
Answer – The points will be posted the day before the RFP closes.

27. Question - Does the scope include advising and strategic planning support for the technologies listed?
Answer – The scope may include advising and strategic planning support, depending on the specific project.
28. Question - What will be the engagement model for Vendors that are awarded this contract? Will JMU issue statements of work for the selected vendors to compete? Will the statements of work be for hourly staff augmentation or will it also include fixed price strategic engagements? Can you provide additional information on the anticipated level of collaboration and coordination between the successful bidder and JMU IT staff?
Answer – As information technology consulting needs arise, the University will contact a firm(s) on contract to discuss the project for which the University requires assistance. A statement of work will be requested from the vendor based on contract terms and pricing, and additional discussions will occur.
29. Question - What will be the maximum number of awardees under this contract? Please confirm the anticipated number of awards.
Answer – The University does not have an anticipated or maximum number of awards for this RFP.
30. Question – For this RFP, are resources expected to be on-site or remote in Harrisonburg, VA? Given the skill sets, we're assuming it's fully remote, but wanted to verify
Answer – Remote is usually acceptable; however, it would depend on the nature of the engagement.
31. Question - How many users are on Office 365? What license do they have? Provide a license count.
Answer – Approximately 30,000 accounts. The majority have A5 licenses with a few having A3 licenses.
32. Question - Are the licenses being purchased directly with Microsoft or through a Microsoft Partner?
Answer – SHI.
33. Question - Do you currently use Microsoft Teams and/or Microsoft SharePoint?
Answer – Yes.
34. Question - Is there a software in place currently to manage endpoints remotely? If so, what product(s) are being used?
Answer - JAMF Pro, Microsoft Intune, and Microsoft Endpoint Configuration Manager are used.
35. Question - How often are the devices and endpoints being updated? Monthly/quarterly/etc. basis?
Answer – Endpoint patches are deployed typically the same month they become available.
36. Question - Do you have employees working remotely that use a company device?
Answer – Yes.
37. Question - Do you offer Bring Your Own Device (BYOD) to employees?
Answer – No.
38. Question - Is there a Mobile Device Management (MDM) solution deployed?
Answer – Yes, for JMU owned devices.

39. Question - How many desktops/laptops/mobile devices are you supporting?
Answer – JMU IT actively manages roughly 4,500 Windows devices, 2,500 Mac devices, and 1,000 mobile devices.
40. Question - Which version of Windows are the desktops/laptops running on?
Answer – Primarily Windows 10 22H2.
41. Question - Are user devices being backed up? If so, how often, and do you have retention policies in place?
Answer – User devices are not centrally backed up.
42. Question – Are the servers on-site or on the cloud? Hybrid?
Answer - Servers are onsite.
43. If you have a cloud environment, is it Azure/AWS/other?
Answer – The University has applications in both Azure and AWS.
44. Question - How many servers do you have? What operating system are they on? Do you have any Windows Server 2012/2012R2? Any Linux Servers? Microsoft is sunsetting Windows 2012 servers in October. Is there a plan to upgrade/replace your current 2012 servers? Please provide details.
Answer – The University has approximately 500 servers. Windows and Linux.
- **2012R2 (26 servers - all slated to decom by October, with the potential exception of 3 belonging to Card Services, which they handle on their own and are in discussions with IT-Sec about)**
 - **2016 (89 servers)**
 - **2019 (93 servers)**
 - **2022 (7 servers)**
 - **Linux (210 Servers) primarily running RHEL 7 & 8**
 - **16 - VMware Host servers, and 3 management servers, running VMWare version 7. (13 normal hosts, 3 VDI hosts, 2 VCenter servers and the VRealize server)**
 - **54 - additional servers are being tracked, but are either security servers (OS not maintained by us), Other Linux (CentOS) or OVAs (Virtual appliances)**
45. Question - Is there a Disaster Recovery plan in place? What is the infrastructure at the fail over location?
Answer - Yes. Disaster Recovery plans exist for critical systems. There is geographical, power, and HVAC redundancy at the failover location, as well as off-site backups in the event of whole data center loss.
46. Question - How many databases are you using? Please specify which ones.
Answer – See RFP Section II. Background.
47. Question - What are some of the critical applications being used today? Any ERP applications?
Answer – See RFP Section II. Background.
48. Question - What is the network topology currently used, and how are these locations communicating to each other?
Answer - On campus locations are serviced via single mode fiber. Off campus locations are a combination of DIA circuits and wireless bridges.

49. Question - Is there a VPN in place for remote access? Is there a firewall?
Answer - Yes to both.
50. Question - What is the speed of the network connection to the internet? Do you have a backup connection?
Answer - Two 8Gbs pipes in active/active state.
51. Question - How many Routers, Switches, and Firewalls are in your network?
**Answer - L2 switches: 855
L3 switches/routers: 10
Firewalls: 4**
52. Question - How many buildings/locations?
Answer – The University has approximately 185 buildings on 750 acres. The campus is divided by interstate 81 and the C&P railroad.
53. Question - How big is your current IT department, if any?
Answer - Approximately 150 employees
54. Question - Please provide the brand for the switches, network devices, laptops, desktops, and printers.
**Answer - Cisco Routers and switches for the wired network. The wireless network is Aruba.
Laptop/Desktops are a mix of Dell and Apple. Printers vary, but a significant number are leased KM Bizhub devices.**
55. Question - Do you have any cameras to support?
Answer: Yes. Cameras are managed by Facilities Management.
56. Question - Do you currently have a VOIP solution? Who is your VOIP provider? What is the brand of your desktop phones? How many extensions/DID numbers?
Answer – The University is currently deploying an NEC VoIP solution with Black Box Network Services, and have approximately 8,000 user and service type extensions. Phones are NEC.
57. Question - Do you have ticketing system in place? Estimate of tickets per month/quarter?
Answer - Yes. The University uses Cherwell as its ITSM ticketing system and receives approximately 49,189 tickets per year.
58. Question - Do you require someone to be on-site all the time?
Answer - That would depend on the nature of the engagement.
59. Question - Is this a multi-vendor or single vendor award?
Answer – This is anticipated to be a multi-award contract.
60. Question - Is there Change Management system in place?
Answer - Technical hardware or software changes are managed through the University's ITSM.
61. Question - Is there an Information Technology Asset Management (ITAM) solution in place?
Answer – Not as such. The University uses Cherwell ITSM for CMDB, and JAMF Pro and Intune for MDM.

62. Question - What applications are currently in use?

Answer – See RFP Section II. Background.

63. Question - The RFP has some focus on Salesforce in the opening. But I see that Huron was awarded a contract for Salesforce work less than 6 months ago. Is JMU looking to understand other options that can support the Salesforce deployment if needed?

Answer – Yes, the University is interested in other Salesforce resources and skillset augmentation options.

64. Question – Are there any pain points of issues with the current vendor(s)?

Answer – No.

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



August 3, 2023

ADDENDUM NO.: Two

TO ALL OFFERORS:

REFERENCE: Request for Proposal No: **RFP# FDC-1175**
Dated: **June 15, 2023**
Commodity: **Information Technology Consulting Services**
RFP Closing On: **Tuesday, August 15, 2023, at 2:00 p.m.**

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

1. Question - How far along is the Reengineering Madison project? When is the new system expected to go live?
Answer - See RFP Section II. Background.
2. Question - Can you please share the portfolio of projects/initiatives that will be executed under the Reengineering Madison program?
Answer - See RFP Section II. Background.
3. Question - Can you provide ticket volumes that you are currently experiencing for PeopleSoft for the last one year, preferably by severity?
Answer - No. Ticket volume alone is not a good indicator.
4. Question - What is the size of the existing support team supporting PeopleSoft?
Answer - 10 people.
5. Question - Will existing support team members be moved to the Reengineering Madison project?
Answer - Yes, in part.
6. Question - Can you provide the architecture diagram for your PeopleSoft application and its deployment?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
7. Question - What is the current PUM level for each of the PeopleSoft application pillar?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
8. Question - What is the number of environments that exist for each PeopleSoft application pillar (example - DEV, TEST, DMO, UAT etc.)?
Answer - 4 environments.

MSC 5720
752 Ott Street, Room 1042
Wine Price Building
Harrisonburg, VA 22807
Office of 540.568.3145 Phone
PROCUREMENT SERVICES 540.568.7935 Fax

9. Question - What is the size of the production database for each of the PeopleSoft application pillar?
Answer - This information may be provided depending on the engagement and after the execution of a SOW.
10. Question - Does Oracle Core Technologies mean the Oracle DBA skill set? If not, please provide more details.
Answer - Yes.
11. Question - What skills are required in Desktop and Mobile Device Management?
Answer - Required skills, certifications, or qualifications will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP Section IV.3.).
12. Question - Please provide details of the services expected in the following technologies:
a. Security and Federation Services
b. Microsoft 365 (M365)
c. Audio and Visual Technologies
d. Secure Research Enclaves
Answer - Services may vary depending on the nature of the engagement.
13. Question - What is expected from Svcs and Cert in Change Management? What are the roles of Senior Engineer/Engineer in Change Management?
Answer - See RFP Section IV. Statement of Needs and Section D. Pricing Schedule. If your firm refers to a specific role by a different name, list it in the space provided next to the corresponding role.
14. Question - Does onsite pricing refer to work specifically performed on campus (in person), and does offsite work pertain to work conducted within the US but off-campus, remote?
Answer - Yes.
15. Question - What positions are you looking to fill immediately? Is there current or future project you are expecting?
Answer - See RFP Section II. Background.
16. Question - For onsite services, we find that a base billable rate is suitable for most of our clients, and hotel/travel expenses charged as actuals later. Would you still like a single blended hourly charge for these positions including all expenses?
Answer - Yes.
17. Question - What are the Oracle core technologies focused on consulting services like OBIA, OBIEE, ODI, OAC, etc.?
Answer - Unavailable at this time.
18. Question - Is there a preferred cloud provider like AWS, GCP, or Azure for a data lake/data warehouse solution?
Answer - No.
19. Question - Is the data warehouse/data lake solution in place that required migrating to a new tool stack or a new solution is expected?
Answer - See RFP Section II. Background.

20. Question - Is there a preferred visualization tool for analytics?
Answer - No.
21. Question - Has Fluid UI been implemented in your PeopleSoft Application?
Answer - No.
22. Question - Is the Boomi atom/molecule installed on-premises or in the cloud?
Answer – On-premises.
23. Question - What Salesforce modules have been implemented/utilized?
Answer - Implementation is just beginning. See RFP Section II. Background.
24. Question - Is it mandatory to showcase the amount of sales our company had during the last twelve months with each VASCUPP Member Institution? Can we skip this portion if we do not have an existing/ previous VASCUPP cooperative contract? Will the proposal be deemed non-responsive if we do not have sales during the last twelve months with each VASCUPP Member Institution?
Answer - A response to the question is required. If the answer is none/zero, indicate that as your answer. Previous sales/experience with a VASCUPP Member Institution is not a requirement for submitting a proposal or being awarded a contract.
25. Question - Please confirm whether the "Secure Research Enclave" category includes CMMC readiness testing? Or, is this category meant for the development/implementation of the architecture for these enclaves?
Answer - Secure Research Enclave could include CMMC readiness or the development/implementation of the architecture for these enclaves.
26. Question - How does JMU define "Consulting Services" and "technology advisor"?
Answer - See RFP Section IV. Statement of Needs.
27. Question - Is this a new requirement or an existing requirement?
Answer - This RFP is to replace an existing contract with multiple vendors.
28. Question - What are your Key Performance Indicators?
Answer - Key performance indicators will vary depending on the project.
29. Question - If we have a teaming agreement with a subcontractor, does the subcontractor's experience count as experience for us?
Answer - The experience of a subcontractor specified in a proposal may be considered in the evaluation of the qualifications and experience of the Offeror.
30. Question - Do we need to submit only one response including the price schedule?
Answer - Vendors should submit one (1) original and four (4) copies, and electronic copy in WORD format or searchable PDF (on a flash drive) of the entire proposal, INCLUDING ALL ATTACHMENTS. The original, copies, and electronic version should all be the same and include the pricing schedule.

31. Question - As a firm registered on eVA, do we have to pay the fees before the submission of the proposal (i.e. this stage) or after award? Please also clarify that the subcontractor also has to pay this fee.
Answer - eVA fees are only paid upon receipt of a purchase order issued through the eVA system. eVA fees are paid by the vendor listed on the issued purchase order. If a subcontractor is issued a purchase order directly, they would have to pay the associated eVA fees; however, if the purchase order is issued to the prime contractor, and the subcontractor is working under the prime contractor, the subcontractor would not pay the associated eVA fees. The University typically issues purchase orders to the prime contractor.
32. Question - Do we need to submit provided RFP Cover Sheet as a Cover Page of the proposal?
Answer - The RFP cover sheet does not need to be submitted as the cover page of a proposal.
33. Question - Is there any local preference for this contract?
Answer - No.
34. Question - Is it mandatory to have experience with higher education institutions?
Answer - Experience with higher education institutions is not required.
35. Question - Please confirm whether security assessment and consulting services are included on this contract. If so, should we price this under the category "Security and Federation Services" on the Pricing Schedule?
Answer - The scope may include security assessment and consulting services, depending on the specific project. In addition to completing *Attachment D*, Offerors should also provide pricing for all other services.
36. Question - Is there any flexibility in the initial contract duration of one year? Is it safe to assume that the same terms and conditions will remain same when the project is renewed? Are there any pre-defined criteria to be met by the vendors to get the renewal of contract?
Answer - JMU typically issues contracts for one year with subsequent one-year renewals. The terms and conditions of existing term contracts are reviewed at the time of renewal. Contract terms may be negotiated and modified as necessary. See RFP *Section VIII.F*.
37. Question - Can you please specify the list of all technologies in each technology area under Section IV? Example: Do we need to consider Oracle Database, Fusinon Middleware, SOA, BPM, Identity Management, MDM, Webcenter-Sites, Portal, Content, Social, OBIEE, Golden Gate and ODI when you refer to Oracle Core Technologies? Similarly, can you call out all technologies under each area?
Answer – See RFP *Section II. Background*.
38. Question - Can you provide more information about the technologies listed in Section II of the RFP, such as Oracle Core Technologies, PeopleSoft Enterprise Solutions, Microsoft Azure, Okta, etc.? What level of expertise and experience is JMU looking for in these areas?
Answer – The level of expertise and experience required will vary based on the specific project. Offerors should include the qualifications and experience of the personnel who may be assigned to perform work for the University in their proposals (See RFP *Section IV.3*).

39. Question - What are the expected outcomes of the trainings that a vendor needs to provide to the staff? How much training must be provided in a month? What will be the number of attendees in each session? Will it be a virtual or classroom training?
Answer – Training outcomes, frequency, number of attendees, format, etc. will vary depending on specific training needs and agreed upon SOW.
40. Question - Can you provide more details about the weightage or scoring system that will be used to evaluate proposals based on the criteria stated in the RFP? How will the award decision be made?
Answer - See RFP Section IV. Evaluation and Award Criteria. Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time.
41. Question - Can you provide more information on the Virtual Payables options mentioned? How can vendors and suppliers enroll in these options?
Answer - Offerors may contact the JMU Accounts Payable office, at acctspayable@jmu.edu or (540) 568-7397 to discuss payment enrollment options.
42. Question - Please list all the technologies/tools that needs to be replaced/transformed as part of Reengineering Madison program. Are there specific projects the vendor team will be involved if selected?
Answer - See RFP Section II. Background.
43. Question - Does the University anticipate any of its current implementation partners will act as a Systems/Services Integrator and an offeror submitting a proposal in response to this solicitation act as subcontractor if selected?
Answer - No.
44. Question - Are you engaged with any cloud service provider? What is the scope of cloud-based solutions in this RFP?
Answer - See RFP Section II. Background.
45. Question - What are your expectations for the level of service that you would like to receive from the IT consulting firm? How would you measure the success of the IT consulting project?
Answer - Expectations and measurements of success will vary depending on the engagement.
46. Question - What are your expectations for the level of security that you would like to have in place?
Answer - JMU follows the ISO standard. When needed other standards are used depending on the need, regulations, requirements, etc.
47. Question - What are the specific challenges that you are facing with your current IT infrastructure compelling to go through Re-engineering Initiative?
Answer - See RFP Section II. Background.
48. Question - Could you provide more information about the anticipated scope of special projects where the contractor will serve as a technology expert? What are some examples of these projects and their objectives? Can you elaborate the expected deliverables and milestones for the projects covered in the scope this RFP?
Answer - See RFP Section II. Background.

49. Question - Is there any preference for local or regional vendors?

Answer - No.

50. Question - Is it safe to assume that offsite means offshore?

Answer - No. For the purpose of this solicitation, offsite means remote work performed not on campus.

51. Question - Resources working offshore need to align with client working hours as per US time zones?

Answer - Yes.

52. Question - Will JMU provide laptops to the vendor consultants?

Answer - No.

53. Question - Will any additional travel costs be considered in the pricing?

Answer - No. See RFP Section X. Pricing Schedule.

Signify receipt of this addendum by initialing "*Addendum #2* _____" on the signature page of your proposal.

Sincerely,

Doug Chester
Buyer Senior
Phone: 540-568-4272