JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU7144**

This contract entered into this 25th day of March 2025, by Impact Makers, Inc., hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

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

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

PERIOD OF PERFORMANCE: From April 1, 2025 through March 30, 2026 with nine (9) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposal FDC-1220 dated December 17, 2024:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) Addendum One, dated January 10, 2025;
- (e) Addendum Two, dated January 16, 2025.

(3) The Contractor's Proposal dated January 30, 2025 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations Summary, dated March 17, 2025.

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

CONTRACTOR:	PURCHASING AGENCY:
By: Joseph W Pugh, Jr (Signature)	By: (Signature)
Joseph W Pugh, Jr (Printed Name)	Doug Chester (Printed Name)
Title: Executive Vice President	Title: Buyer Senior

Rev. 5/12/21

RFP # FDC-1220
Information Technology Security Auditing Services
Negotiation Summary for Impact Makers, Inc.
March 17, 2025

1. Parties agree that items within this Negotiation Summary modify RFP #FDC-1220 and the Contractor's response to RFP #FDC-1220 and that this Negotiation Summary takes precedence in conflict.

2. Contractor agrees that all exceptions taken within their initial response to RFP #FDC-1220 that are not specifically addressed within this negotiation are null and void.

3. The pricing schedule is as follows:

Pricing for Auditing Services	Off-site	On-site*
External Vulnerability Scanning	$158.98	$180.17
Wireless Network Assessment	$158.98	$180.17
Firewall and Router Security Assessment	$158.98	$180.17
Server Configurations Assessment	$158.98	$180.17
Database Architecture Security Assessment	$158.98	$180.17
Network Scanning Process Assessment	$158.98	$180.17
Web Application Security Assessment	$158.98	$180.17
Active Directory Security Assessment	$158.98	$180.17
Penetration Testing	$250.00	$281.25
Telecommunications	$158.98	$180.17
**** (flat fee hourly rate that includes all billables/travel)***		

4. 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.

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

6. Upon completion of each Statement of Work, the Contractor shall submit a SWaM subcontractor usage report in accordance with RFP Special Term and Condition J: Small Business Subcontracting and Evidence of Compliance. Reports shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu.

7. Contractor has disclosed all potential fees. Additional charges will not be accepted without mutual written agreement between parties, e.g., contract modification and/or change order.

impactmakers

Proposal for

James Madison University

RFP# FDC-1220 – Information Technology Security Auditing Services

January 30, 2025

Table of Contents

RFP Cover Sheet

REQUEST FOR PROPOSAL

RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

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

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

Sealed Proposals Will Be Received Until 2:00 PM on January 21, 2025 for Furnishing The Services Described Herein. (See Special Terms & Conditions "D. Late Proposals")

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

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

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

Name and Address of Firm:

Impact Makers, Inc.

3200 Rockbridge Street, Suite 201

Richmond, VA 23230

By: Scott K Hammer *(Signature)*

Name: Scott K.Hammer *(Please Print)*

Date: January 30, 2025

Title: Vice President Emeritus

Web Address: impactmakers.com

Phone: (804) 306-9685

Email: shammer@impactmakers.com

Fax #:

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 SKH #2 SKH #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

I. Introduction and Executive Summary

Dear James Madison University Information Technology Security Auditing Services Selection Team,

Below this letter you will find Impact Makers' proposal for providing Information Technology Security Auditing Services for James Madison University (JMU) in response to JMU RFP# FDC-1220. Impact Makers' team is prepared to provide all of the services requested in JMU's RFP# FDC-1220.

Why Impact Makers Can Best Support JMU for Information Technology Auditing Services

Impact Makers' team understands the University's need for consulting services to support JMU AMS and IT staff. We believe that we can best support the University because of:

- **Our Approach.** Impact Makers' time-tested approach has proven repeatedly to deliver exceptional results for our clients. We utilize custom documented processes, reusable value-adding tools, and methods enriched with nearly twenty years of lessons learned to ensure successful delivery and best outcomes for our clients.
- **Our Standards.** Impact Makers' IT Security Audit Services conform both to the *International Standards for the Professional Practice of Internal Auditing*, issued by the Institute of Internal Auditors (IIA) and to the *Government Auditing Standards* (Yellow Book standards) issued by the Federal Government Accountability Office (GAO). As required by the IIA and GAO, Impact Makers has conducted quality assurance reviews (QAR) of its IT Security Audit Services through self-assessments followed by independent validations. The independent reviewer found that our IT Security Audit Services generally conform to the IIA standards and receive a rating of "pass" with respect to the Yellow Book Standards. A copy of the independent reviewer's Yellow Book review letter is attached as an Appendix to this proposal.
- **Our Experience.** As a contract holder under the contract pursuant to JMU RFP# FDC-1057, which JMU RFP# FDC-1220 will supplant, Impact Makers has provided IT Security Audit and Assessment Services to a range of higher education clients, including the University as well as the Virginia Military Institute, Norfolk State University, Richard Bland College of the College of William and Mary, Virginia State University, and the Virginia Community College System. We have also provided information security assessments and audits for many other organizations including the Virginia Information Technologies Agency, Virginia Department of Motor Vehicles, Virginia Department of Social Services, Virginia Department of Health, and the Virginia Department of Elections, among others.
- **Our Team.** Our team is seasoned in bringing our approach, expertise, experience, and Information Security knowledge to bear in order to exceed our clients' expectations. Impact Makers' exceptional consultants have deep risk management and IT security experience with specific familiarity with IT security audits and risk management planning and developed the Commonwealth of Virginia (COV) IT Security Audit Standards as well as the COV IT Security Policy, Standard, and Guidelines. In addition, our consultants have delivered information security and risk management projects for multiple higher education institutions, state government agencies, and other organizations.
- **Our Model.** Simply put, our business model is to support the communities in which we work. Since 2006, we have contributed $4.7 million in unrestricted financial support and 11,000+ hours pro bono management and technology consulting services to nonprofit community partners. This unique model attracts top talent, who chose Impact Makers as part of their legacy. Our mission-and-values-aligned team consistently outperforms those only interested in a single bottom-line and bring passion to the transformative work we do for our clients and community partners.

Thank you for considering Impact Makers to meet JMUs needs. We look forward to the opportunity to continue to work with you.

Best regards,

Joseph W. Pugh, Jr.
Executive Vice President
(804) 641-1551
jpugh@impactmakers.com

Scott K. Hammer
Chief Information Security Officer
(804) 306-9685
shammer@impactmakers.com

II. Background and Summary of Understanding

The purpose of this proposal is to respond to the Request for Proposal (RFP) # FDC-1220 to enter into a contract to provide Information Technology (IT) Security Auditing Services for James Madison University (JMU or the University), an Agency of the Commonwealth of Virginia.

Impact Makers understand the needs of the University as listed in Section IV of the RFP. Based on our understanding, the University is seeking qualified firms to provide expertise and a range of services to support technologies used by the University. The University intends these firms to serve on special projects as a technology expert when requested and as needed and to provide reports to the University summarizing options and providing recommendations. In addition, the University is seeking firms to serve as a technology advisor to understand, communicate, and propose solutions as requested and to serve as a resource for research, implementation, troubleshooting, and other technical tasks to support the efforts of JMU IT staff.

In addition, the University is seeking firms to supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit and Management Services to support the IT auditing functions of the University's Audit and Management Services (AMS) organization. This support will include, without limitation, the audits listed below that are currently being performed by University personnel or by the staff of contractors performing under formal statement of work agreements with the University:

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

Impact Makers has the ability to provide all of the services requested by the University through RFP# FDC-1220. Impact Makers will serve on special projects as a technology expert and advisor to understand, communicate, and propose solutions when requested.

III. Approach and Methodology

Impact Makers' approach is to work in a collaborative way that draws on the knowledge and expertise of University staff and augments that knowledge and expertise with our experience and skills. In addition, we will ensure that project deliverables address the relevant business requirements specified by the University.

We will ensure the success of each engagement by managing it using industry-standard project management processes based on the Project Management Institute's Project Management Body of Knowledge (PMBOK), to assure on-time, on-budget delivery of the services that will meet the University's needs. In developing project deliverables, we will also leverage our collective experience managing and reviewing University projects and deliver the project using consultants with specific expertise in Information Security and in the specific disciplines required by each project. With our processes and tools, our experience, and factoring in the unique mission and culture of your organization, we will deliver results that achieve your objectives.

Overall Approach

Impact Makers' general approach to IT Security Audits is depicted in Figure 1, which is further described below:

A. Plan Project. Impact Makers begins each project with a project initiation phase to engage with project stakeholders, confirm project objectives, and develop project governance documents, including the project charter, project plan, and schedule. After developing these documents, Impact Makers will solicit and integrate the organization's feedback on these documents and present the documents in a project kickoff meeting. These project initiation activities ensure consensus between Impact Makers and the University on project approach, timeline, and key deliverables.

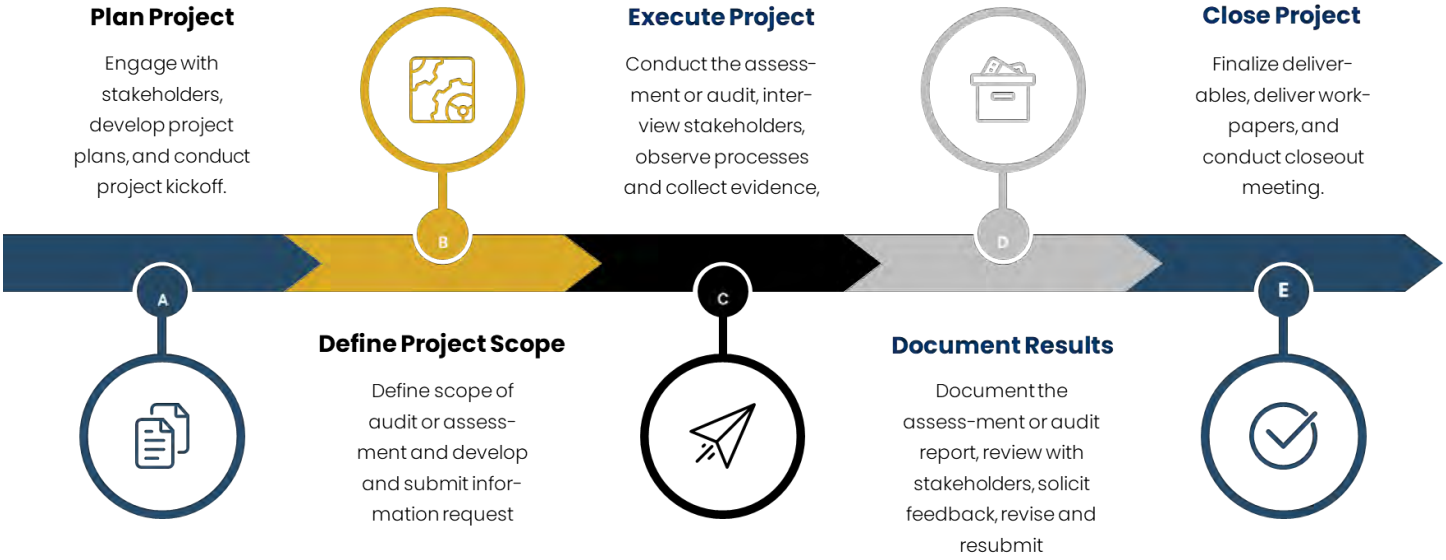

Figure 1 – Impact Makers' IT Security Audits Approach

B. Define Project Scope. Following project initiation activities, Impact Makers will work with stakeholders to define the scope of the audit or assessment, including controls that are specifically within or excluded from the assessment or audit scope. Based on this scope definition, Impact Makers will develop, review with stakeholders and revise, and then submit a comprehensive evidence request for the information needed to conduct the assessment or audit. For tracking and reporting of information requests, Impact Makers will maintain a list of items requested, with item description, date requested, name of requestor, name of responsible staff, due date agreed to, date received, and additional comments.

C. Execute Project. In this phase, Impact Makers will conduct the assessment or audit work that will form the basis for findings and recommendations resulting from the project. During this project phase, Impact Makers will also review and analyze the information requested during the Define Project Scope phase and use this information to inform the need for further information gathering. Based on this determination, Impact Makers will interview personnel, observe personnel executing relevant processes, inspect the results of relevant process execution, and collect evidence of the extent to which information security controls are in place and are effective.

In executing the assessment or audit, Impact Makers will document the results of its work, including, in the case of audits, documenting audit workpapers sufficient to support the work performed and the conclusions reached in the draft reports to be developed as the result of the audits. This documentation will include a detailed list of all controls evaluated and a determination of whether the system under consideration is compliant, non-compliant, or partially compliant with each control, a listing of the audit program step number, the number of the audit point sheet in which the finding

is included (for controls with which a system is non-compliant or partially compliant), a description of the finding, recommendation and the control tested.

In this project phase, Impact Makers will also hold weekly project status and touchpoint meetings. These meetings will include a summary of project status to date, including any potential findings and recommendations.

D. Document Results. In this project phase, Impact Makers will document draft reports of the results of the project and submit them to the project sponsor for review. The reports will detail the scope of the assessment or audit, fieldwork undertaken in conducting the project, and detail project findings and recommendations.

The reports will document findings, recommendations, and overall conclusions. The draft reports will group detailed findings if they share a common subject. Findings in the reports will include easily identifiable elements of a finding: condition, criteria, cause, effect, and recommendation.

Impact Makers will then conduct a review meeting or exit conference in the case of audits. In each review meeting or exit conference, Impact Makers will review findings and draft reports with project stakeholders. Impact Makers will document the review meeting, obtain feedback on the report, and incorporate the feedback in a final report. In the case of audits, Impact Makers will also document and deliver finalized audit workpapers to the project sponsor.

E. Close Project. In this project phase, Impact Makers will bring the project to an orderly close. Impact Makers will document and present to the project sponsor a Project Closeout Presentation, detailing accomplishments, best practices, and lessons learned.

Throughout the project, Impact Makers executes against the project plan and manages the project schedule. We monitor and manage risks, issues, actions, and decisions. Impact Makers provides regular status reports at an agreed-upon cadence. Should a critical issue or risk arise, Impact Makers team will raise it in a timely manner and escalate, as necessary. In this way, we monitor and manage project communications and ensure project quality.

The Impact Makers Advantage

We believe that our security assessment services stand out from the competition due to the experience and approach of our consultants. We have worked on numerous assessments and audits for the University and other Commonwealth of Virginia (COV) institutions of higher education and state agencies, including developing security policies and procedures. For example, members of our team developed the Commonwealth's Information Security Standard, along with associated policies, procedures, and guidelines, and we leverage this experience to develop structured tools that facilitate the audits and assessments we perform. Typically, the guidelines provide very detailed, organized assessment methodology, but Impact Makers' tools allow us to approach them efficiently, demonstrate the validity of the assessment, and provide traceability to the captured data and evidence.

As noted in the Introduction and Executive Summary, above, Impact Makers has provided Information Technology Security Audit and assessment services to a range of higher education clients, including the University as well as Virginia Military Institute, Norfolk State University, Richard Bland College of the College of William and Mary, Virginia State University, and the Virginia Community College System. We have also provided information security audits and assessments for many other organizations including multiple state agencies such as the Virginia Information Technologies Agency, Virginia Department of Motor Vehicles, Virginia Department of Social Services, Virginia Department of Health, the Supreme Court of Virginia, and the Virginia Department of Elections, among others.

In addition, as already noted, Impact Makers' IT Security Audit Services conform both to the International Standards for the Professional Practice of Internal Auditing, issued by the Institute of Internal Auditors (IIA) and to the Government Auditing Standards (Yellow Book standards) issued by the Federal Government Accountability Office (GAO). As required by the IIA and GAO, Impact Makers has conducted a quality assurance review (QAR) of its IT Security Audit Services through self-assessments followed by independent validations. The independent reviewer found that our IT Security Audit Services generally conform to the IIA standards applicable to providing audit services to clients and that our IT Security Audit Services generally conform to the Yellow Book Standards.

Impact Makers has also partnered with Rattlesnake Creek LLC, a Virginia Department of Small Business and Supplier Diversity (SBSD)-certified small and micro business to deliver the proposed services to the University. Rattlesnake Creek is a leading provider of information security assurance, audit, and assessment services to public sector clients and will assist Impact Makers in delivering high-quality IT Security audit and assessment services to the University and other VASCUPP members while assisting the University in meeting its SWaM goals.

Service Delivery Methodology

The section below is our plan and methodology to provide services in areas a) through j) as listed above and in the Section IV of the University's RFP. These plans and methodologies address the requirement in Section V, Paragraph B, Item #2 of the University's RFP. Each of our assessments follow the general outline depicted in Figure 1, above. In particular, the Plan Project and Close Project phases are very similar across the University's requested services. We detail how we execute the Define Scope, Execute Project, and Document Results steps for each of the proposed services below.

A. External Vulnerability Scanning

Vulnerability scanning is a vital component to an organization's information security program. Impact Makers utilizes vulnerability scans to provide a "moment in time" view of the network security posture, which can be used as inputs into many more other areas within an information security program by utilizing industry-standard frameworks, such as NIST 800-53 and 800-37, CIS, PCI 3.1, and HIPAA, to deliver comprehensive vulnerability assessments. Impact Makers goes beyond providing assessment results, working hand-in-hand with our clients to formulate a sound, strategic, and measurable response for the remediation of identified vulnerabilities. We take a phased approach towards conducting vulnerability assessments.

1. **Define Scope.** Defining the scanning scope, including any specific targets for evaluation, schedule, and points of contact for the engagement ensures that the results of the project will meet the University's needs. During this process, we confirm the requirements to ensure that our assessment process delivers the desired goal. We confirm the system boundary and appropriate times and guidelines for conducting the assessment.

2. **Execute Project.** Utilizing industry standard tools such as Nmap, Nessus, and OWASP's Zed Attack Proxy (ZAP), the Execute Project phase begins with a system discovery to determine hosts that are alive and network accessible. The tools probe the systems to identify the host type, operating system, running services, and other pertinent information, allowing Impact Makers to gain a sense of the network topology. Upon completion of the network discovery, we conduct a comprehensive evaluation of the organization's systems, scanning all network IP addresses to identify, quantify, and classify potential system weaknesses. Where applicable, we incorporate the use of system credentials to thoroughly interrogate the system to discover the system security level. We employ tools and plug-ins that will examine open ports, protocols, services, configuration, applications, and patching levels of the system to evaluate the results against common security best practices and known

vulnerabilities. Given sufficient credentials, systems can be interrogated to determine compliance with applicable frameworks if desired.

3. **Document Results.** Once the systems have been evaluated and the data captured, we perform data analytics to provide insightful reports on the relevant vulnerabilities and associated risks to include severity, priority, and remediation recommendations. We correlate the assessment findings to known vulnerability databases such as CVSS, as well as security controls found in common cyber security frameworks such as NIST 800-53, Center for Internet Security (CIS), HIPAA, and PCI 3.1, to classify risk severity and priority. We then develop and present a report of our assessment results to leadership. The report will contain recommendations for next steps and best practices to help remediate any findings and strengthen the University's security posture.

B. Wireless Network Assessment

Impact Makers' methodology for wireless technology assessment includes the following steps.

1. **Define Scope.** In the planning phase, the Impact Makers team works with organization personnel, as appropriate, to identify the scope of existing wireless infrastructure and physical areas to be included in the assessment, and to establish rules of engagement. This phase does not include any actual testing but sets the groundwork for a successful test.

2. **Execute Project.** In the Wireless Network Assessment phase, we typically execute the following steps:

    a. **Site Survey** – In this phase, a wireless scanning tool, such as Kismet, is used to scan for available wireless access points and related metadata within the physical assessment scope, and to parse the results.

    b. **Results Analysis** – We analyze the results of the wireless site survey for metadata, factors such as cipher, observed signal strength, ESSID, MAC address, Privacy type, authentication type, channel, and approximate location.

    c. **Follow-up Testing** – Depending on the observed network types, we perform follow-up testing. Such testing may include, without limitation:

        i. Man-in-the-middle ("Evil Twin AP") attacks
        ii. Capturing and brute forcing the 'handshake' to determine passphrase
        iii. Validating segmentation between 'guest' and private internal networks
        iv. Validating access restrictions in place on 'guest' networks
        v. Sniffing (intercepting) traffic to and from unencrypted access points
        vi. MAC address spoofing

3. **Document Results.** Based on the results of the site survey and testing, we issue a report detailing results and recommendations for any observed weaknesses. Our report includes considerations such as use of lightweight APs, appropriate segmentation and connectivity between wireless networks, and the locations of potential rogue access points.

In addition to the listed attributes, we also include cipher, authentication type, privacy type, and observed signal strength. Further, based on the results of the testing, we may recommend testing segmentation between guest networks and any private internal network, testing other access restrictions on guest networks, and intercepting traffic between client and AP on unencrypted wireless networks to determine the nature of that traffic and its potential risk.

C. Firewall and Router Security Assessment

The Impact Makers' approach to assessing firewall and router security includes the following steps.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of the current environment by collecting evidence such as network diagrams, firewall rules, baseline documentation, etc.

2. **Execute Project.** Our team will assess the environment based on the following key areas:

   a. Physical Security – As part of the assessment, Impact Makers assesses the ability for individuals to physically gain access to routers. This assessment also includes analyzing the cables that connect devices to and from the network to prevent unauthorized access such as port sniffing or a similar malicious attack.
   b. Logical Access – We assess who has access to these devices to ensure that only individuals who need access to perform their job responsibilities have access.
   c. Configurations – Impact Makers assesses the configurations of these devices based on best practices. These configurations may include:
      i. Approved ports and services
      ii. Inbound and outbound traffic
      iii. Anti-spoofing rules

3. **Document Results.** Based on the results of the testing, Impact Makers issues a report detailing results and recommendations for any observed weaknesses and vulnerabilities. Our report is typically organized based on the highest risk areas and will include recommendations in order to resolve those findings.

D. Server Configurations Assessment

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of current server configurations, including baseline hardening standards, server configuration items (CIs), and other data. Based on this data, we develop a detailed plan for conducting the assessment.

2. **Execute Project.** Impact Makers utilizes the Center for Internet Security (CIS) benchmarks in order to assess server configurations based on the following areas:

   - User Configuration – Impact Makers assesses user access to the server to make sure that the risk of inappropriate access is mitigated.
   - NTP Configuration – Impact Makers gains an understanding of the Network Time Protocol (NTP) in order to prevent 'time-drift' for Linux based servers.
   - SSH – Impact Makers inspects SSH protocol versions and configuration to ensure administrative sessions remain private.
   - Hardening Standards – Impact Makers assesses the environment against the University's baseline requirements for hardening standards and verifies that system configuration standards are appropriately implemented.
   - Logging & Monitoring – Impact Makers ensures that activities are logged & monitored appropriately.

3. **Document Results.** Based on the results of the assessment, Impact Makers issues a report detailing results and recommendations for any areas where server configurations depart from baseline standards and best practices. Our report is typically organized based on the highest risk areas and will include recommendations in order to resolve those findings.

E. Database Architecture Security Assessment

Impact Makers leverages The Open Group Architecture Standard (TOGAF) and National Institute of Standards and Technology (NIST) standards in performing database architecture security assessments.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of the current database architecture.

2. **Execute Project.** Our team assesses the environment based on the following key areas:

   a. Logical Access – Impact Makers assesses who has direct database access to ensure that only individuals who need access to perform their job responsibilities have access.
   b. Connection Points – Impact Makers will gain an understanding of the connection points to better understand data egress and ingress including potential data loss risks.
   c. Sensitivity of Data – Impact Makers determines the sensitivity and data classification of data in the database to determine the appropriateness of access and configuration controls.
   d. Security Configurations – Impact Makers will review security configurations including, but not limited to, encryption, tokenization, backups, and access controls.

3. **Document Results.** Based on the results of the testing and feedback from relevant stakeholders, Impact Makers develops recommendations on future state architecture. Our report is typically organized based on the highest risk areas and includes recommendations in order to resolve those findings. Along with the recommendations, Impact Makers provides a high-level roadmap that includes the network and security components to be implemented in a meaningful way, the required resources, costs to implement, and possible organizational changes that need to occur to operationalize these components.

F. Network Scanning Process Assessment

Impact Makers understands that a Network Scanning Process is important both for troubleshooting and for system security. Organizations need to understand the full range of devices connected to the network in order to effectively monitor for potential vulnerabilities. In providing these assessments, Impact Makers seeks to gain an understanding of the existing network scanning process and compare the current state to best practices based on industry standards.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of the current network scanning process.

2. **Execute Project.** Our team assesses the current network scanning process against industry standards such as SEC530, NIST800-53, or other specified by the University, with a focus on control objectives and on scanning-related controls such as those in the NIST800-53 AC, AU, CM, MP, PL, RA, SC, and SI control families.

3. **Document Results.** Based on the results of the assessment, Impact Makers develops recommendations to improve the network scanning process, as needed, to meet control objectives and conform to relevant best practices and guidance. Our report is typically organized based on the highest risk areas and includes recommendations in order to resolve those findings. Along with the recommendations, Impact Makers provides a high-level roadmap that includes the frequency and type of scans to be performed and plans to implement process changes.

G. Web Application Security Assessments

Impact Makers understands the significance of Web Application Security Assessments. Impact Makers' objective of these assessments is to evaluate applications within the context of the University's business, to leverage knowledge of approved information security designs and methodologies, and to identify weaknesses in application design.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of the web applications to be assessed and any areas of emphasis for the assessment.

2. **Execute Project.** Impact Makers utilizes a variety of automated and manual auditing techniques to perform the different application risk assessments required by the University. In each of these types of testing, however, we follow similar steps, as outlined below:

    a. For white box testing we use a blend of openly available code quality scanners to identify issues in the application code base.
    b. For black box testing we use both opensource and commercial scanners to interrogate both the application and the infrastructure components within the system boundary.
    c. For grey-box testing, many of the same tools are used from the black-box testing, but we focus on automated software testing techniques that involve providing invalid, unexpected, or random data as inputs (e.g., fuzzing techniques) specific to the known application context.

3. **Document Results.** Based on the results of the assessment, Impact Makers develops recommendations to improve web application security. Our report is typically organized based on the highest risk areas and includes recommendations in order to resolve those findings. Along with the recommendations, Impact Makers provides a high-level roadmap that prioritizes the recommendations and outlines plans to implement the recommendations.

H. Active Directory Security Assessment

Impact Makers understands that one of the most serious threats organizations face is the use of Active Directory configurations to identify attack paths and capture privileged credentials so that attackers can deeply embed themselves into the organization's networks. Our Active Directory Assessment Services are designed to identify vulnerabilities in the organization's Active Directory implementation and to provide recommendations to remediate those vulnerabilities.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment and gains an understanding of the organization's Active Directory infrastructure and any areas of emphasis for the assessment.

2. **Execute Project.** Impact Makers assesses Microsoft Active Directory (AD) in the following areas:

    a. AD forest and domain trust configurations
    b. Domain controller management review including operating system (OS) versions, patching, backup, and server lifecycle management
    c. Domain controller auditing configuration
    d. Administration groups (e.g., users, service accounts) with a specific focus on groups with privileged access to AD
    e. Organizational unit (OU) permissions with a focus on top-level domain OUs

3. **Document Results.** Based on the results of the assessment, Impact Makers highlights AD security misconfigurations and recommends specific remediation/mitigations that may include identifying specific event IDs (domain controller auditing, overall Windows system) that should be logged and monitored.

I. Penetration Testing

The Impact Makers' approach to network penetration testing is based upon recommendations from both the National Institute of Standards and Technology Special Publication (NIST SP) 800-115 (Technical Guide to Information Security Testing and Assessment) and the Open Source Security Testing Methodology Manual (OSSTMM).

As outlined by NIST, and departing slightly from our approach for other services, our high-level penetration testing methodology involves four key phases, which may all occur remotely.

1. **Define Scope.** In the Define Scope phase, the Impact Makers' team works with organization personnel, as appropriate, to identify the test objectives, identify the scope, determine attack vectors and establish rules of engagement. The level of awareness and type of test to be performed (black box vs. grey box vs. white box) will also be determined. This phase does not include any actual testing but sets the groundwork for a successful penetration test.

2. **Discover.** During the Discover phase, Impact Makers uses appropriate tools (such as Maltego, Nmap, and Nessus) and techniques to gather information required for the various attack vectors. From a network perspective, this includes, but may not be limited to, the following:

    a. Performing reconnaissance activities, both manual and automated, to discover external-facing assets and IP addresses
    b. Conducting network foot-printing and probing for active devices
    c. Performing port scans of systems to identify potential entry points and fingerprint operating system versions and listening services / applications
    d. Searching the Internet and public information sources for information leakage to determine whether any sensitive information can be discovered and leveraged in the attack phase
    e. Conducting vulnerability scans to identify vulnerabilities present on the network and applications that may present attack vectors

3. **Attack.** During the Attack phase, the Impact Makers' team integrates and analyzes the information gathered in the previous phases. We develop an attack plan that includes prioritized options for exploiting identified vulnerabilities. If provided advance detail about the environment, tests may be tailored to focus on high-impact endpoints.

    With approval and under the supervision of the University's management sponsors, the Impact Makers' team executes the attack plan using permitted vectors. Depending on the vulnerability and exploit used, successful access may or may not be in the form of privileged access. If the exploit results in unprivileged access, Impact Makers' team will attempt to perform privilege escalation by exploiting one or more additional vulnerabilities.

    The initial attack and penetration may result in access to a given system, but not necessarily access to one that is business critical or that contains sensitive information. In this case, we may attempt to "pivot" on the compromised platform and attempt to identify and compromise another target by repeating the previous steps, but from the perspective of the already-compromised system. Throughout this phase, testing techniques will also be used to attempt detection evasion and test the effectiveness of malicious activity monitoring and alerting solutions.

At the end of the attack phase, the Impact Makers' team works with the organization to clean up the actions that have been performed during the penetration test, so that any compromised systems are returned to their original state.

During the course of the attack phase, the Impact Makers' team will leverage one or more of the following core tools:

a. Kali Linux – penetration testing distribution
b. Metasploit – open source penetration testing framework
c. Burp Suite – platform for performing security testing of web applications
d. Zed Attack Proxy – proxy for performing web application testing
e. Wireshark – network packet capturing tool
f. Ettercap – toolset for Man-in-The-Middle (MiTM) attacks

4. **Document Results.** Based on the results of the testing, Impact Makers issues a report detailing results and recommendations for any observed weaknesses and vulnerabilities. Our report is typically organized based on the highest risk areas and includes recommendations in order to resolve those findings.

J. Telecommunications

Impact Makers understands that universities conduct telecommunications audits for several key reasons, including identifying and eliminating unnecessary expenses, ensuring that the university is not overpaying for telecommunications services and ensuring that all telecommunications services and contracts comply with relevant regulations and internal policies. In addition, universities perform these audits to assess the efficiency and effectiveness of current telecommunications services, identifying areas for improvement or upgrades, to evaluate the need for new technologies or infrastructure that can enhance communication and operational efficiency, and to identify and mitigate any security vulnerabilities within the telecommunications infrastructure.

Impact Makers' Telecommunications audit services are designed to address any or all of these drivers and to help the University maintain a robust, cost-effective, and secure telecommunications environment, supporting its overall mission and operational goals.

1. **Define Scope.** Our team works with organization personnel to define the scope and goals of the assessment.

a. Identify Objectives – Determine the primary goals of the audit, such as cost reduction, compliance verification, or service optimization.
b. Inventory Assessment – Compile a comprehensive list of all telecommunications assets, including devices, services, and contracts.
c. Stakeholder Engagement – Involve key stakeholders to understand their needs and expectations from the audit.

2. **Execute Project.** Impact Makers collects and analyzes all relevant data.

a. Data Collection – Gather all relevant data, including invoices, contracts, usage reports, and service agreements.
b. Data Analysis
   - Billing Errors – Check for discrepancies in billing, such as incorrect charges or double billing.
   - Usage Patterns – Analyze usage data to identify underutilized or overutilized services.
   - Contract Compliance – Ensure that all charges align with the terms of the contracts.

c. Optimization – Identify opportunities to optimize service plans, eliminate redundant services, and negotiate better rates with vendors.

3. **Document Results.** Based on the results of the assessment, Impact Makers will create a detailed report summarizing the findings, including identified errors, cost-saving opportunities, and recommendations for optimization. We will also work with the University to develop an action plan to implement the recommended changes, including timelines and responsible parties, as well as a plan for regular follow-ups to ensure that the recommended changes are implemented.

IV. Expertise and Qualifications

The section below is a written narrative statement to address the expertise, qualifications, and prior experience of the firm, as well as a sample of resumes of specific personnel to be assigned to perform the work, to address the requirement in Section V, Paragraph B, Item #3.

A. Relevant Experience

As noted above, Impact Makers has worked with several Commonwealth of Virginia institutions of higher education to conduct IT security assessments and audits under the terms of contract pursuant to JMU RFP# FDC-1057, which JMU RFP# FDC-1220 will supplant, including:

- James Madison University
- Norfolk State University
- Richard Bland College of the College of William and Mary
- The Virginia Community College System
- Virginia Military Institute
- Virginia State University

We have also provided services to the following Virginia colleges and universities using other contracts:

- The College of William and Mary
- George Mason University
- Radford University
- University of Virginia Health System
- Virginia Commonwealth University Health System
- Virginia Tech

In addition, we also have delivered consulting services to more than two dozen Commonwealth of Virginia agencies as well as other organizations, providing consulting and security assessments and audits for:

- Bon Secours Health System
- Donate Life Virginia
- Library of Virginia
- Supreme Court of Virginia
- University of Virginia Health System
- Virginia529 College Savings Plan
- Virginia Alcohol Beverage Control
- VCU Health System
- Virginia Employment Commission
- Virginia Department of Aviation

- Virginia Hospital and Healthcare Association
- Virginia Department of Behavioral Health and Disability Services
- Virginia Department of Corrections
- Virginia Department of Education
- Virginia Department of Environmental Quality
- Virginia Department of Elections
- Virginia Department of Health
- Virginia Department of Motor Vehicles
- Virginia Department of Planning and Budget
- Virginia Department of Social Services
- Virginia Department of Taxation
- Virginia Department of Transportation
- Virginia Indigent Defense Commission
- Virginia Information Technologies Agency
- Virginia State Corporation Commission
- Virginia State Police

State-supported colleges and universities and state agencies have unique challenges that often include limited resources, including staffing, time, and budget and can extend to employee engagement, cumbersome business processes, regulatory environments, disparate data or access issues, lack of buy-in, or other obstacles. Impact Makers is experienced with these and many more challenges and often finds that preparation, communication, and organizational change management can smooth the road to executing the project and reporting results that are most useful to our higher education and public sector clients. In particular, we would draw your attention to the client success stories that are in the Appendix of this proposal.

B. Certifications

Impact Makers' security team members hold the following certifications:

- Certified Information Systems Security Professionals (CISSP)
- Certified Information Systems Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information System Controls (CRISC)
- Governance, Risk, and Compliance Certification (CGRC)
- CompTIA Security+
- Project Management Professional (PMP)
- Scaled Agile Framework (SAFe)
- Six Sigma Green Belt
- ITIL Foundation

Impact Makers' continuing education program includes ongoing training, conferences, and other opportunities for Continuing Professional Education (CPE) and Continuing Professional Development (CPD). Additionally, we offer internal knowledge transfer, on-the-job training, study groups to assist with new certifications, support, and guidance.

C. Project Qualifications

The project descriptions that follow detail projects that Impact Makers has delivered to clients in response to requests similar to the services requested in JMU RFP# FDC-1220.

1. Norfolk State University – IT Security Assessments

Impact Makers conducts IT security assessments of several of NSU's critical, sensitive applications.

Founded in 1935, Norfolk State University (NSU) has grown over the years into an independent HBCU with university status, serving more than 5,000 students. In furtherance of its mission, NSU deploys many Information Technology (IT) systems and engaged Impact Makers to conduct security assessments of several of these systems.

The Challenge

NSU was recently granted additional operational authority by the Virginia General Assembly, and, under this authority, needs to conduct security assessments of its sensitive technology systems. As an agency of the Commonwealth of Virginia (COV), NSU is subject to information security requirements promulgated by the Virginia Information Technologies Agency (VITA). Among these requirements is that agencies must conduct a risk assessment of any IT systems classified as sensitive at least once every three years.

In order to ensure that the required assessments were effective, NSU engaged Impact Makers to conduct security assessments of Ellucian Colleague, the NSU ERP, and DMS OnBase, its document sharing system. In addition to assessing risks against VITA requirements, NSU also wanted to gauge its compliance with the Graham-Leach-Bliley Act (GLBA) and the Federal Education Rights and Privacy Act (FERPA). After completing this first group of assessments, NSU extended Impact Makers' engagement to include its Guardian, CAD/RMS, and ATS systems.

Impact Makers' Solution

Impact Makers first documented and described the overall NSU technology environment in which the systems operate. After characterizing the systems and their environment, we conducted and documented an analysis of the system against relevant controls.

After conducting this controls analysis, we identified and documented threats and vulnerabilities to which the systems are subject and how the threats and vulnerabilities combine to form specific risks. We also documented the likelihood and impact of each risk identified, as well as an overall rating of the risk based on likelihood and impact.

Based on this analysis, we documented the overall risk matrix for the systems. This matrix included the threat and vulnerability, the specific risk that the threat and vulnerability combine to create, correlation of the risk with the controls analysis and other relevant factors, the risk likelihood, impact, and overall risk rating, and recommendations for the treatment of each risk.

After the assessments were finished, we completed the security assessment report, submitted it to NSU for review, and solicited feedback on the assessment. We then revised the assessment as required and submitted it to NSU for final approval.

Our Client's Successes

The assessments Impact Makers conducted highlighted a number of risks for NSU:

- Risks associated with the overall NSU IT environment in which the systems operate, and
- Risks associated with the individual systems assessed.

A number of these risks, particularly those associated with the NSU technology environment, were items of which NSU was already aware. The NSU information technology organization had not been able to focus University executive management on these risks, though, and the assessment by Impact Makers assisted in obtaining this management focus. An essential element in obtaining this focus was the specific, actionable risk mitigation recommendations included in the security assessment reports.

Based on the success of this effort, NSU extended Impact Makers' engagement to conduct security assessments of three additional IT systems and to improve its contingency plans.

2. Virginia Military Institute (VMI) System – IT Security Assessments

Impact Makers assesses the compliance of controls supporting several of VMI's critical, sensitive applications.

The Virginia Military Institute's (VMI) applications support the operation of the Institute. As such, sensitive information is obtained, generated, stored, processed, and transmitted. Ensuring adequate protection of this sensitive information is critical to the mission of the Institute.

The Challenge

In furtherance of its mission, VMI deploys many Information Technology (IT) systems; among these systems are the Ellucian Colleague Enterprise Resource Planning (ERP) system and the Software Etrieve electronic forms system. As an agency of the Commonwealth of Virginia (COV), VMI is subject to the IT Security requirements promulgated by the Virginia Information Technologies Agency (VITA). Among these requirements is that agencies must conduct a risk assessment of any IT systems classified as sensitive at least once every three years.

As systems that handle sensitive data, both the Colleague ERP system and the Etrieve electronic forms system are classified as sensitive. To meet VITA requirements and to provide assurance that it is protecting these systems commensurate with sensitivity and risk, VMI requested information security assessments of these two systems.

Impact Makers' Solution

To assist VMI in meeting these objectives, Impact Makers conducted IT security assessments of the systems to ensure compliance with both SEC501-11.4 and with the COV ITRM IT Risk Management Standard (SEC520-03). We finalized plans for the assessments during project initiation in collaboration with VMI and obtained VMI approval of the plans. We then conducted each assessment.

In each assessment, we described the overall VMI technology environment in which the subject system operates, and characterized the system, including function, location, system and data owner, and system boundary. We also documented system interfaces, interconnections, the sensitivity of each type of data handled by the system and overall system sensitivity.

We then conducted and documented an analysis of the system against the controls included in SEC501-11.4. This analysis included a description of the control, whether the control is in place, not in place, or planned, and the extent to which the control mitigates risks to the system.

After conducting the controls analysis, Impact Makers documented threats and vulnerabilities to which each system is subject and how the threats and vulnerabilities combined to form specific risks. We then documented the likelihood and impact of each risk identified, as well as an overall rating of the risk based on likelihood and impact.

Our Client's Successes

Our assessments identified risks that may otherwise not be realized. We ensured that the Institute's systems are implemented with the requisite controls in place and fully supported. Furthermore, in areas that increased risk to the organization, we highlighted those risks, provided background information, provided recommended solutions and ramifications to accepting the risks rather than remedying or mitigating them.

3. Virginia Community College System – IT Security Assessments

Impact Makers helps the Virginia Community College System evaluate its IT security program and identify areas for enhancement.

The Virginia Community College System (VCCS) oversees a network of twenty-three community colleges in Virginia, which serve residents of Virginia and provide two-year degrees and various specialty training and certifications. In 2006, the Virginia Community College System's annual enrollment rate topped 233,000 students.

The Challenge

Within VCCS, Information Technology Services (ITS) provides centralized Information Technology (IT) services, along with IT oversight and guidance. While ITS provides information security oversight and guidance and provides Information Security Officers (ISOs) to some of the colleges, ITS does not have granular control over how information security controls are applied and managed. As a result, while the colleges often indicate that they are meeting VCCS central office information security requirements, such as multi-factor authentication, these assertions have not been confirmed.

To bridge these gaps, VCCS Internal Audit engaged Impact Makers to conduct IT Security Assessments of several VCCS member colleges. VCCS Internal Audit's overall objective for these assessments is not only to identify individual issues, but also to evaluate holistically whether the information security program is being implemented effectively at each college and is achieving its intended control objectives.

Impact Makers' Solution

To assist VCCS in meeting these objectives, Impact Makers conducted IT security assessments of five VCCS member colleges selected by the VCCS Internal Audit. Prior to beginning the assessments, we worked with the VCCS Internal Audit Director to design an assessment program, which is based on VCCS information security requirements and Center for Internet Security (CIS) guidance and is designed to provide the holistic assessment that VCCS is seeking.

In this approach we conducted each assessment, then conducted a retrospective with VCCS Internal Audit and the Impact Makers team after each assessment, to capture best practices and lessons learned, and to provide continuous improvement by integrating these elements into the subsequent assessments. In addition, to maximize the value provided by these assessments, Impact Makers adopted a risk-based approach of limited spot-checking of controls that the in-scope colleges assert they have in place. This approach replaced the more extensive testing based on statistical sampling we would normally conduct in a full-fledged audit to provide the more holistic assessment sought by VCCS. In addition, at VCCS' request, we limited the scope of the assessments to focus on key areas and used Center for Internet Security (CIS) guidance to guide the assessments.

Our Client's Successes

VCCS has gained the holistic assessment of whether the information security program is being implemented effectively at each college and is achieving its intended control objectives. Based on this assessment, VCCS is planning for corrective actions to remediate gaps discovered. In addition, VCCS has re-engaged Impact Makers to conduct additional, similar IT security assessments.

4. Virginia State University – IT Security Audits

Impact Makers helps Virginia State University identify control weaknesses and meet COV requirements.

Virginia State University (VSU), founded in 1882, is one of Virginia's two land-grant institutions and is a public, comprehensive 1890 Land Grant institution and historically Black college/university. It is committed to the preparation of a diverse population of people through the advancement of academic programs and services that integrate instruction, research, extension, and outreach. The University endeavors to meet the educational needs of students, graduating lifelong learners who are well equipped to serve their communities as informed citizens, globally competitive leaders, and highly effective, ethical professionals.

The Challenge

Although it is an educational institution, VSU is subject to Commonwealth of Virginia (COV) information security requirements, including the requirement that all sensitive IT systems receive an IT Security Audit not less than once every three years. VSU has frequently relied on Impact Makers to conduct these audits, and on this occasion engaged Impact Makers to conduct IT Security Audits of its network infrastructure and of its Kronos time and attendance system.

Impact Makers' Solution

Impact Makers conducted the requested IT Security Audits, gathering information, conducting fieldwork, and documenting findings and recommendations. Impact Makers identified several areas where VSU was able to take actions and improve control effectiveness to meet its control objectives.

Our Client's Successes

As a result of the IT Security Audits, VSU met COV information security requirements. In addition, VSU improved control effectiveness in several areas and addressed several outstanding audit points from the Auditor of Public Accounts.

5. Richard Bland College – Third-Party Controls Assessment Evaluation

Impact Makers helps Richard Bland College determine the adequacy of information security controls deployed by its third-party Software-as-a-Service (SaaS) providers.

Richard Bland College is a public junior college associated with the College of William and Mary and is located in Prince George County, Virginia. Richard Bland College was established in 1960 by the Virginia General Assembly as a branch of the College of William and Mary under the umbrella of "the Colleges of William and Mary". Richard Bland has continued as a junior college of the College of William and Mary.

The Challenge

Richard Bland College ("the College") obtains many of its IT systems via Software-as-a-Service (SaaS) from third party providers. The College had accepted the representations of the third-party SaaS providers that the providers' information security controls were adequate to protect the confidentiality, integrity, and availability of the College's data, and the College had not evaluated these controls independently.

To implement information risk management best practice and to meet VITA requirements, the College needed to conduct an independent review of the third-party SaaS providers' information security controls. Because it did not have sufficient internal resources to conduct this assessment itself and based on Impact Makers' reputation for conducting this sort of assessment effectively and efficiently, the College engaged Impact Makers to conduct the assessment.

Impact Makers' Solution

Impact Makers obtained SOC2, Type 2 reports from each of the three third-party SaaS vendors to be assessed. We then reviewed each report against the requirements of SEC501-11.3 and SEC525-4.1 to identify where each report documented compliance with or departure from the requirements of the relevant standard.

After conducting the review of each SOC2, Type 2 report, Impact Makers documented an evaluation report. The evaluation report detailed where each vendor's SOC2, Type 2 reports documented compliance with or departure

from the requirements of the relevant standard. After documenting the reports, we reviewed them with the College, obtained feedback from the College, and revised the reports accordingly.

Our Client's Successes

Impact Makers worked with the College to identify areas where each of its third-party SaaS vendors did or did not comply with the requirements of SEC501-11.3 and SEC525-4.1. Based on this assessment, the College was able to request control improvements from its third-party vendors. These control improvements will both ensure adequate protection of the confidentiality, integrity, and availability of the College's data, and enable the College to demonstrate compliance with the relevant VITA information security standards.

6. Virginia Department of Taxation – IT Security Audits

Impact Makers helps the Virginia Department of Taxation conduct IT Security Audits of a key system and of its general IT security controls.

Virginia's Department of Taxation (VATAX) serves the public by acting ethically and efficiently in administering Virginia's tax laws. It seeks to be the leading tax administration agency through a customer-first focus and culture based on accountability, collaboration, and trust. With increasing online tax filing and an ever-changing cyber threat environment, auditing VATAX systems for cybersecurity systems is of critical importance.

The Challenge

As part of its IT Audit program, VATAX complies with VITA/ITRM requirements to perform IT audits on sensitive systems commensurate with risk and at a minimum of once every three years. To assist in meeting these needs, VDSS required a SEC501- and SEC525-compliant audit of its Computer Assisted Collections System for Government ("CACSG"), a software application that routes delinquent debts/cases through various collection states based on predefined business rules and procedures. In addition, to eliminate the need to evaluate common/general controls in each IT Security Audit of its many sensitive systems, VATAX wanted to conduct an overall IT Security General Controls Audit. To meet these needs, VATAX engaged Impact Makers to conduct these audits.

Impact Makers' Solution

Impact Makers used the methodology proposed for the contracted VATAX IT Security Audits to identify common and system-specific controls, evaluate the common controls once, and evaluate the system-specific controls for the CACSG system. Using this methodology, Impact Makers conducted an IT Security Audit of the CACSG system and of general/common IT Security controls, conducted audit fieldwork, identified findings, documented audit reports, presented the reports to management, revised the reports based on feedback, and documented an overall Corrective Action Plan, Final Audit Report, and Exit Conference documentation.

Our Client's Successes

Impact Makers successfully helped VATAX identify key gaps in control effectiveness for the CACSG system and for a number of its key general controls and a plan to bridge these gaps. Based on executing the Corrective Action Plan documented by Impact Makers, VATAX has improved its information security compliance and aligned management of its IT systems with its risk appetite.

7. Virginia Department of Social Services – IT Security Audits

Impact Makers helps the Virginia Department of Social Services conduct IT Security Audits of numerous systems.

Virginia's Department of Social Services (VDSS) has a budget of over $1.8 billion dollars. VDSS protects Virginia's most vulnerable citizens by ensuring they have access to critical lifesaving services. VDSS ensures delivery of these services by

providing oversight and guidance to 120 local offices across the state serving over 1.6 million Virginians each year.

The Challenge

As part of its IT Audit program, VDSS complies with VITA/ITRM requirements to perform IT audits on sensitive systems commensurate with risk and at a minimum of once every three years. To assist in meeting these needs, VDSS needed SEC502.2-compliant audits for twelve of its sensitive systems. VDSS turned to Impact Makers, the Commonwealth of Virginia security provider of choice, for help in conducting these audits.

Impact Makers' Solution

Impact Makers identified common and system-specific controls, evaluated the common controls once, and evaluated the system-specific controls for each in-scope system. Using this methodology, Impact Makers conducted IT Security Audits of the twelve in-scope systems, conducted audit fieldwork of the systems, identified findings, documented audit reports, presented the reports to management, revised the reports based on feedback, and documented an overall Corrective Action Plan, Final Audit Report, and Exit Conference documentation.

Our Client's Successes

Impact Makers successfully helped VDSS identify key gaps in control effectiveness for a number of its mission essential systems and a plan to bridge these gaps. Based on executing the Corrective Action Plan documented by Impact Makers, VDSS has improved its information security compliance and aligned management of its IT systems with its risk appetite.

As a result of the successful delivery, VDSS has continued to engage Impact Makers in completing risk assessments required to meet SEC501 compliance, assisting them with developing their risk assessment process and training VDSS staff on conducting SEC501 required risk assessments.

8. Virginia529 – IT Security Audits

Impact Makers helps Virginia529 identify control weaknesses and meet COV requirements.

Virginia529 started in 1994 when the Virginia General Assembly authorized a program to help citizens save for the increasing costs of higher education. One of the earliest 529 plans formed, the Virginia Higher Education Tuition and Trust Fund—which evolved into Virginia529—began offering a prepaid tuition plan in 1996. Over the next twenty years, one program expanded to offer customers additional choices.

Now available nationwide with account owners in every state, Virginia529 is the nation's largest 529 plan, managing over $62 billion in assets.

The Challenge

As a program sponsored by the Commonwealth of Virginia, Virginia529 is required to develop an information security program that includes assessing the risks associated with its sensitive IT systems, conducting IT Security Audits of these systems no less frequently than once every three years. To assist it in meeting these requirements, Virginia529 engaged Impact Makers to conduct IT Security Audits of the following three systems:

1. Pitney Bowes First (PB First) system provides the proprietary address validation system that is used to ensure that Virginia529 mailing addresses are accurate.
2. Expression Engine system is a newly rolled out application that supports Virginia529's Achieving a Better Life Experience (ABLE) Savings program.
3. SOAR, an Oracle database that collects account data for SOAR scholars and applicants. The applications sit on a physical Linux server where VA529's primary enterprise system, Banner, also resides.

Impact Makers' Solution

Impact Makers conducted the requested IT Security Audits, gathering information, conducting fieldwork, and documenting findings and recommendations. Impact Makers identified several areas where Virginia529 was able to take actions and improve control effectiveness to meet its control objectives.

Our Client's Successes

As a result of the IT Security Audits, Virginia529 met COV information security requirements. In addition, Virginia529 improved control effectiveness in several areas.

D. Consultant Resumes

The resumes that begin on the next page are representative of the staff that Impact Makers would assign to Statements of Work issued pursuant to the contract resulting from the University's RFP. Impact Makers would assign staff to each engagement based on the requirements of the engagement, the input of the University, and the availability of staff members.

Scott K. Hammer, PMP, CISM, CRISC — Principal Consultant

Professional Background

Scott Hammer is Impact Makers' Chief Information Security Officer and leads Impact Makers' internal security program and its delivery of cybersecurity and information risk management services to clients He has 35+ years of experience in local, state, and Federal government, higher education, non-profit organizations, financial services, and retailing in many specific areas of expertise, including:

- Information Technology Resilience, Security, and Risk Management
- Organizational transformation and strategic planning
- Human Capital Management
- Business Process Assessment, Design, and Improvement
- Program and Project Management
- Business Continuity Planning
- Information Technology Assessment and Audit
- Information Technology Infrastructure Design, Implementation, and Management
- E-Commerce
- Information Technology Architecture and Strategy Development and Implementation

Professional Experience

Chief Information Security Officer (2022-present)
Vice President, Public Sector Consulting Services (2020-2022)
Public Sector Client Partner (2019-2020)
Principal Consultant (2016-2018)

Impact Makers, Inc., Richmond, VA

- Led development of multiple risk assessments for Norfolk State University and for Richard Bland College. Project included documenting risks, their likelihood and impact, and making recommendations for their mitigation.
- Led development of cybersecurity incident response plan for the Virginia State Corporation Commission (SCC). Project including assessing incident response needs, developing processes and procedures to meet identified needs, and developing and conducting a tabletop exercise to test the plan.
- Led development of a Disaster Recovery-System Availability Plan for Chesterfield County. Project included developing inventory of the County's IT applications and their recovery requirements and documenting plans to meet the requirements. Project also including developing and conducting a tabletop exercise to test the County's ability to respond to and recover from a disruption.
- Led cybersecurity assessment project for the Virginia Department of Elections. Project included documenting Business Impact Analysis (BIA), Risk Assessments (RAs), Business Continuity Plan (BCP), and IT Disaster Recovery Plan (IT DRP). In addition, project led to actionable recommendations to improve agency business resilience, including establishing an agency COO position, which the agency implemented.
- Led a transformational information security project for the Virginia Department of Motor Vehicles. Project included developing BIA, twenty-six sensitive system RAs, BCP, and IT DRP. In addition, project assisted in developing business 50+ IT and business processes to enhance the agency's security posture and build a culture of security in the agency and move the agency to a service management framework for service delivery.
- Led critical infrastructure protections cybersecurity assessment of the operational technologies (signals and other traffic management devices) against the Commonwealth of Virginia SEC501 standard and other relevant frameworks. Project led to actionable recommendations to improve the cybersecurity of these devices to enable connected vehicle and other advanced traffic technologies.
- Led an assessment of current and potential future uses of technology for the Virginia Department of Corrections to assist the agency increase security and employee productivity and achieving long-term cost savings. The assessment

documented technological innovations which could be applied to current and future prisons and to the supervision of offenders in the community and enable more effective decision-making on technology investments.
- Led security audits of sensitive IT systems for Virginia State University. Project enabled identified key control weaknesses in these systems enabling the University to identify and prioritize needed mitigation, as well as enabling the University to meet compliance requirements.
- Led self-assessment of Impact Makers' IT Security Audit Services against Institute of Internal Auditors Red Book requirements. Facilitated independent review of the self-assessment. The independent reviewer found that our IT Security Audit Services generally conform to the IIA standards applicable to providing audit services to clients.
- Led development of agency Business Impact Analysis (RA) and Risk Assessments (RAs) for the Virginia Department of Health. Project also analyzed agency information security policies and provided role-based information security training that enabled the agency to improve its security posture and comply with state information security requirements.

Principal Consultant
The North Highland Company, Richmond, VA (2004-2016)

- Led a diverse team of consultants and client personnel in developing enterprise-wide information technology (IT) security policies, standards, and guidelines for the Commonwealth of Virginia. This project enabled the Commonwealth to provide consistent IT security across its enterprise and enabled the Commonwealth's IT strategy for consolidation of IT infrastructure.
- Led consulting teams that assisted more than a dozen Commonwealth of Virginia agencies in the development of Business Impact Analyses, Risk Assessments, Business Continuity Plans, and IT security policies, processes, and procedures to provide adequate IT security for their businesses and to comply with statutory and regulatory mandates.
- Facilitated developing consensus among the executive team of a public-sector retirement agency regarding the agency's essential business functions. Used this consensus in leading a team of consultants in developing a business impact analysis (BIA), risk assessment (RA), and business continuity recommendations for the agency. This work enabled the agency to focus its business continuity efforts on essential business functions that require recovery within the first 30 days following a disruption.
- Led a consulting team in development of a business continuity plan for a state retirement agency. Derived recovery requirements from a business impact analysis and developed alternative approaches for recovery of essential business functions and supporting resources and business processes. Obtained client approval of preferred approach and led development of a fully executable business continuity plan, including detailed recovery procedures.

Managing Consultant
Netstar-1, Rockville, MD (2002-2004)

- Developed the information security architecture and assurance program for a cabinet-level Federal agency. Improved information security compliance by instituting industry best-practice policies, processes, and procedures. Insured ongoing security compliance that enabled the agency to achieve a grade of "B" on the Federal Computer Security Report Card, the fourth-highest grade received by any cabinet-level Federal agency.

Senior Director, Directory and Messaging Services
Capital One, Richmond, VA (2001-2002)

- Managed six direct reports, total staff of fifty-seven, and budget of $5M. Provided continuous availability of messaging environment, timely completion of network administration work orders, and effective directory security management. Reduced directory security violations from 850 to eight in six months, protecting Capital One's information resources. Team received a Circle of Excellence award for this work.

Vice President, Network Services
SunTrust Bank, Richmond, VA (1994-2001)

- Managed six direct reports, total staff of thirty operating budget of $75M, and annual capital projects totaling $35M. Coordinated strategic technology planning with corporate business strategy and managed planning and engineering for a data, voice, and video network with over 1,300 sites and improved network reliability to 99.99% through key process and technical improvements.

Computer Systems Engineer
The College of William and Mary, Williamsburg, VA (1989-1992)

- Managed the college academic computing system and networks, serving over 7,000, students, faculty, and staff.

Systems Engineer/IT Director
The Commonwealth of Virginia, Richmond, VA (1985-1989; 1992-1994)

- Managed Intranet, Internet, Extranet, desktop, server, and mainframe infrastructures and applications. Managed mainframe and network infrastructure.

Education and Certifications

M.A., B.A., English, State University of New York, Binghamton, NY
Project Management Professional, PMI
Certified Information Security Manager, Certified in Risk and Information System Controls, ISACA
Six Sigma Green Belt, Oriel, Inc.

Community Involvement

Board Member and Immediate Past Chair, The Cultural Arts Center at Glen Allen
Board Member Emeritus and Past Board Chair, The Podium Foundation
Board Member and Senior Strategic Advisor, Richmond Culture Works
Co-founder and Artistic Director, The Shady Grove concert series
Virginia Chapter Past President, ISACA

Gary D. Wills, CISSP, CISM, CISA — Lead Consultant

Professional Background

Gary Wills is a Lead Consultant in Impact Makers' Cybersecurity and Risk Management practice. He is an operational risk manager and IT leader who navigates ambiguity and shifting landscapes to drive profitable change in the financial services sector. Gary strengthens operational efficiency and modernizes business through new ways of working. He cultivates workplace cultures where teams feel empowered to perform at their best. His core competencies include:

Program Design • Team Leadership • Risk Governance • Issue Management • Risk Assessment
IT Audit • Metrics Reporting • Communication • Relationship Building

Professional Experience

Lead Consultant, Cybersecurity and Risk Management
Impact Makers, Inc., Richmond, VA, April 2021 – Present

- Worked closely with the Co-CEO and Public Sector Vice President to enhance the company's Information Security, Risk Management, and Data Governance, Management, and Privacy service offerings.
- Delivered data governance and information security assessment services to a variety of clients across several industry verticals.

Senior IT Operational Risk Manager
Genworth Financial, Richmond, VA, February 2019 – March 2021

Partnered with the business and IT to perform risk assessments to evaluate controls and risks across enterprise systems. Used NIST 800-53 framework to evaluate risks across all domains such as change management, access control, network security, encryption, logging and reporting, and data loss prevention.

- Led a project with executive IT and business teams to evaluate cloud security risks and controls and developed a corporate-wide cloud risk appetite.
- Evaluated the third-party management process and implemented changes to align the process to NIST, ensuring a more consistent evaluation process where all control gaps were documented and consistently reported.
- Evaluated first line supplier processes related to contract management, financial viability, technology, and business operations.
- Documented findings and made recommendations for process improvements across the enterprise.
- Reviewed third parties for controls across all NIST domains, including reviews of SOC 2 reports.
- Developed both internal and supplier metrics (KRIs and KPIs) for board level reporting to effectively demonstrate risk levels.

Vice President and Third-Party Security Leader
Synchrony Financial, Richmond, VA, December 2014 – February 2019

Stood up the third-party security assessment program for a $30 billion bank to align to NIST and FFIEC frameworks to meet regulatory requirements from the Federal Reserve and OCC.

- Hired a team of four onshore and two offshore employees and five contractors to perform 350+ assessments per year. Developed a comprehensive onsite program to ensure suppliers met security and regulatory requirements.
- Performed risk assessments for third parties to evaluate controls in all areas of information security including cloud controls, network and data security, access control, software development, change control, physical security, and PCI compliance.
- Presented finding and risks to ELT and risk committees as needed.
- Provided information security leadership to ensure the third-party program met key compliance requirements for GDPR and new California privacy laws.
- Implemented and integrated Bitsight into the third-party program to provide deeper insight into supplier controls.

- Led the program to implement an online GRC tool (Keylight) to facilitate assessments and improve metrics and quality of the assessment program.
- Evaluated remediation plans and closure details to ensure risks were adequately addressed.
- Partnered with sourcing and the business to streamline the assessment process, improve the escalation procedures, and make reporting more accessible and understandable for the company.
- Led the collaboration with other internal security teams to ensure the assurance, incident response and third-party monitoring teams are sharing information to improve overall security posture at our suppliers.

Capital Audit Team Leader / Lead Supplier Auditor

General Electric, Richmond, VA, March 2012 – December 2014

Led a team of two auditors and five contractors to assess the risks and controls at over 900 third party suppliers per year. Worked with internal stakeholders and suppliers to identify and remediate information security control gaps.

- Participated in the development and implementation of the risk profile, assessment questionnaire and issue management process for assessing third-party suppliers.
- Developed a database to track, monitor and report on over 3,000 assessments and 35,000 identified issues. Led meetings to report on the department's progress to senior IT management.
- Developed relationships and identified contacts to roll out third-party assessment process to Asia Pacific and India. Worked with local IS and purchasing leaders to assess IS controls at 150+ Asia Pacific suppliers in 3 months.
- Performed onsite supplier assessments for high-risk suppliers to identify security gaps.

Senior Internal IT Auditor

Phillip Morris USA, Richmond, VA, October 2006 – March 2012

- Led audit teams to perform IT audits on external vendors and internal applications, infrastructure, and processes. Developed audit plans, assessed process risk, assigned resources, and worked with the business to ensure audit findings were accurate.
- Participated as the IT expert on integrated business process and vendor audits.
- Identified issues in the areas such as Change Management, Data Storage and Transmission, Segregation of Duties and User and Administrative Access, and worked with business management to develop actions plans to remediate the risk.
- Utilized ACL and Microsoft Excel to analyze large quantities of data to identify risk areas for large vendors and processes such as medical prescriptions, payroll, transportation, and revenue.
- Worked on the annual risk assessment team to determine high risk business areas for future audits.
- Produced a data analytics database to facilitate the training and use of data analytics in the audit department.
- Built a database to automate the segregation of duties review for three instances of SAP, which saved the department over 500 person-hours of work each year.

Debt Systems Group Leader

Ford Motor Corporation, Dearborn, MI, May 2003 – October 2006

Led support team for the Global Treasury Management (GTM) system, which tracks, pays, and values over $150 billion in debt and securities for Ford Motor Credit.

- Managed an 8-month project to reengineer how data was sent to the general ledger.
- Reduced workload by 500 person-hours by collaborating with customers to improve system processes and controls.
- Ensured the GTM application met all Sarbanes-Oxley requirements by performing security and controls testing and developing new application control review documentation and network diagrams. Utilized ACL and Microsoft Excel to analyze large quantities of data to identify risk areas for large vendors and processes such as medical prescriptions, payroll, transportation, and revenue.

Education

- MBA, MIS and E-business concentrations, Purdue University, West Lafayette, IN
- BS, Electrical Engineering, Purdue University, West Lafayette, IN

Olusola Fajana, CISA, CompTIA Security+ Senior Consultant

Professional Background

High achieving leader with experience in designing, developing, implementing, and enforcing security requirements. With 6 years + experience preparing Security Test and Evaluation plans. I provided certification and accreditation support (assessment & authorization). Experience developing system security plans, contingency plans, artifacts, and POAMs. I am familiar with developing, testing, and integrating security tools as well as configuring and installing the tools. I am skilled in conducting security audits and developing mitigations to identified risks and conducted vulnerability assessments.

Professional Experience

Cybersecurity Consultant – ISSO

Impact Makers, Inc., Richmond, VA, October 2021 – Present

- Served as the Package Submitting Office (PSO) for Authority to Operate (ATO) package accreditations.
- Assisted in technical documentation review, assessment, and feedback of Risk Management Framework (RMF) packages including POA&Ms, Nessus scans, artifact repository management, and Information Assurance (IA) Controls
- Coordinated security measures including analysis, evaluation, verification, accreditation at appropriate classification level.
- Ensured Cybersecurity architectural artifacts are in compliance while meeting federal National Institute of Standards and Technology (NIST) 800 regulatory requirements for Confidentiality, Integrity, Availability, Authentication, and Authorization of federal IT systems.
- Provided technical and programmatic Information Assurance Services, which include RMF A&A, internal and external customers in support of network and information security systems.
- Designed, developed, and implemented security requirements and artifacts within an organization's business processes.
- Prepared the security documentation from information obtained from customers, using guidelines IAW NIST 800-53, SEC 525, SEC 501, IC, and DISA (Risk Management Framework A&A).
- Prepared the security test plans, assessment and authorization (A&A) support in the development of system security and contingency plans.
- Conducted complex risk and vulnerability assessments of security controls, overlays, and POAMs. Evaluated, developed, and enhanced security requirements, policy and tools, against Federal/State laws and regulations.
- Provided recommendations for closing risk assessments and vulnerability gaps.
- Recommended system enhancements to improve security risk and deficiencies IAW POAM validation. Developed, tests and integrated computer and network security tools.
- Secured system configurations and installs security tools, performed system scans in order to determine compliancy, report results, and evaluates products.
- Collaborated with and support ISSMs, and engineering teams.
- Conducted program security audits and develops solutions to lessen identified risks.
- Developed strategies to comply with privacy, risk management, and e-authentication requirements. Provided information assurance support for the development and implementation of security architectures to meet new and evolving security requirements.
- Provided assistance in computer incident investigations.
- Performed vulnerability assessments including development of risk mitigation strategies.

Cybersecurity Analyst – ISSO

Virginia ABA, Richmond, VA, September 2017 – October 2021

- I was responsible for working in a 24x7 Security Operation Center (SOC) environment.
- Provided analysis and trending of security log data from a large number of heterogeneous securities devices.
- Provide Incident Response (IR) support when analysis confirms actionable incident.
- Provided threat and vulnerability analysis as well as security advisory services.
- Analyzed and responded to previously undisclosed software and hardware vulnerabilities.
- Coordinated the accreditation and delivery of the assembled enterprise data capabilities across all platforms and perform continuous monitoring of the fielded solutions.
- Worked with CDF Platform / systems engineers to remediate security defects in a timely manner on any open findings for all development, test, and production systems.
- Monitored ACAS and CMRS weekly reports, Information Assurance Vulnerability Alerts (IAVAs), Cyber Tasking Orders, and vendor announcements for alerts and forward relevant alerts to the Operations and Maintenance teams for mitigation and response.
- Prepared necessary documentation to describe the protection and sustainment of the IA requirements and support for the DoD Public Key Infrastructure (PKI) implementation strategies.

Senior Help Desk Technician

Institute of Public Health, Ife Osun, Nigeria, August 2006 – September 2017

- Maintained workstation/laptop operational baselines through established processes and procedures.
- Worked as Hardware support, troubleshooting, integration, configuration, and installation of authorized hardware software and peripherals.

Certification and Education

Certified Information Security Auditor (CISA)
CompTIA Security+
Bachelor of Science, Obafemi Awolowo University, Ife Osun, Nigeria
Associate Degree of Education, College of Education, Ekiti - Nigeria

---

Joshua Brannon — Consultant

Professional Background

Highly motivated and positive individual with great organizational and communication skills. Customer service expert and efficient problem solver. Deftly manage administrative functions of the practice. Provide thorough answers and solutions and provide an exceptional customer experience.

Professional Experience

Information Security Consultant
Impact Makers, Richmond, VA, May 2023 – present

- Conducted risk assessments and information security audits for clients including the Virginia Department of Health, the Virginia Employment Commission, and Norfolk State University.

Cyber Security Analyst
CISO Global, Inc., Texas, May 2021 – January 2023

- As Security Analyst, I collaborated with client staff and management to perform risk assessments, GAP assessments PCI Audits and GRC (Governance, Risk and Compliance).
- Managed time budgets for client projects assigned to me.
- Review customer documentation.
- Perform risk assessments based on NIST Cyber Security Framework (CSF) and other agreed framework(s).
- Worked on clients GRC (Governance, Risk and Compliance) programs using various frameworks (NIST CSF, HIPAA, PCI DSS 3.2, and others).
- Wrote and supported policy and procedure documentation in support of client's GRC programs.
- Communicated effectively and efficiently with client staff and management.
- Performed PCI DSS audits and drafted reports for both SAQs and ROCs clients.
- Managed Knowbe4 platform for phishing campaigns on behalf of multiple clients.
- Managed Knowbe4 platform for user education/training for users who failed phishing test and for annual security training.

Cyber Security Engineer
CGI Federal, Inc., Texas, July 2018 – May 2021

- As a Cyber Security Engineer, I handled working Cyber Security Architects and subject matter experts in relationship to assessing, designing, implementing, administering, and maintain enterprise security solutions in environments that were required to adhere to NIST Special Publication 800-53r5 and Special Publication 800-171.
- Help assist with Cyber Security subject matter expert / architect when assessing, designing, implementing, administering, and maintaining enterprise security solutions in an environment subject to NIST special publications 800-53 and 800-171.
- Evaluate the impact of proposed new or updated systems on existing security controls or the overall enterprise security posture.
- Respond to real-time request security-related problems or issues that cannot be resolved by the service desk.
- Document and track client service requests to resolve any issue that would ensure uninterrupted client service.
- Collaborate with other stakeholders to understand needs, evaluate risks, educate, and offer recommendations related to security.
- Assist in validating that technical controls are operating as intended.
- Trend Micro subject matter expert for Anti-Malware on all Linux Server from the Deep Security Manager Console and Deep Security Agents.

- Do required upgrades for all Trend Micro Deep Security Agents and Deep security Console for FIPS Compliance.
- Engineered, maintained, and repaired security systems and programmable logic controls.
- Monitored use of data files and regulated access to protect secure information.
- Monitored computer virus reports to determine when to update virus protection systems.
- Updated quality control standard methods and procedures to meet customer SLA and compliance requirements.

Education

- Keller Graduate School of Management Colorado Springs, CO • 2013
  Master of Business Administration

- DeVry University Colorado Springs, CO • 2012
  Bachelor of Science, Computer Information Systems

Joseph R. Kruger — Associate Consultant

Professional Background

Joseph Kruger is an Associate Consultant in the Risk Management Cybersecurity field. He brings a pro-active, critical thinking approach to his work. He has extensive knowledge of the Project Management side of Business and is currently in the process of obtaining a certificate in accounting.

Business Management • Team Leadership • Accounting • Problem Solving • Risk Assessment
Project Management • Communication • Relationship Building

Professional Experience

Associate Risk Consultant, Cybersecurity and Risk Management
Impact Makers, Inc., Richmond, VA, April 2023 – Present

- Assisted in performing IT audits and risk assessments.
- Reviewed documentation and assessed control strengths.
- Conducted IT risk assessments for Norfolk State University and Richard Bland College and IT security audits for the Virginia Department of Elections and the Virginia Employment Commission.

Education

- BS, Business Management, Hilbert College, Hamburg, NY
- AS, Criminal Justice, SUNY Erie Community College, NY

Sonja Ayers — Associate Consultant

Professional Background

Sonja Ayers is an associate consultant in Impact Maker's Risk and Resiliency practice. She has strong analytical and interpersonal skills with a hardworking approach to overcoming any challenges. She has a solid understanding of information security and risk controls. Her core competencies include:

IT Audit • Communication • Team Oriented • Problem Solving • Detail Oriented • Risk Assessment

Professional Experience

Associate Consultant
Impact Makers, Inc. (June 2024 – Present)

- Developed request lists and reviewed documentation for IT systems based on the NIST and SEC530 frameworks.
- Evaluated documentation to determine if system controls were in place.
- Created workpapers to document my control analysis, ensuring they align with Yellow Book auditing standards.
- Worked with clients to create report formats that ensured findings and observations were adequately documented and understood.

Key Employee – Manager on Duty
Richmond Country Club (January 2020 – Present)

Assisted the General Manager and Food & Beverage Director with operational oversight and inventory. Ensure high standards of customer service, addressed member complaints, and enhanced members' dining experience.

Executive Assistant
Civitas Health Services, Inc. (May 2017 – July 2023)

Acted as a liaison for the CEO, facilitating communication between Program Managers, clinical staff, and external stakeholders. Prioritized delegated tasks and managed deadlines effectively. Handled sensitive information with discretion in a dynamic work environment.

Education

Bachelor of Science in Psychology, Virginia Commonwealth University, Richmond, VA

Additional Education:

- IBM and ISC2 Cybersecurity Specialist Professional Certificate
- Cybersecurity Foundations Certificate
- Cybersecurity Risk Management Framework Certificate

V. Offeror Data Sheet

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

   Impact Makers is well positioned to meet these needs as described in our proposal, above.

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

   Years 18 Months 3

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 #
Virginia Department of Motor Vehicles – Information Security Transformation and many other projects	10 years	2300 W. Broad St., Richmond, VA 23219	Lana Shelley Chief Information Officer (804) 367-2635 lana.shelley@dmv.virginia.gov
Norfolk State University – Numerous IT Security Audit and Assessment projects	3 years	700 Park Ave. Norfolk, VA 23504	Faye Monroe-Davis Chief Information Officer (757) 823-2916 sfmonroe-davis@nsu.edu
Virginia Community College System – Campus IT Security Audits	3 years	300 Arboretum Pl # 200, Richmond, VA 23236	Mary Barnett Internal Audit Director (804) 819-4955 mbarnett@vccs.edu
Richard Bland College – Third party risk assessment and several IT system risk assessments	3 years	11301 Johnson Rd, Petersburg, VA 23805	Susan Clair, Ed.D Chief Information Security Officer (804) 726-7153 susan.clair@rbc.edu
Virginia Department of Taxation – IT General Controls and multiple system audits	6 years	P.O. Box 1115. Richmond, VA 23218	David Walsh Internal Audit Director (804) 786-3670 david.walsh@tax.virginia.gov

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

   Impact Makers, Inc. 3200 Rockbridge Street, Suite 201, Richmond, VA 23230

   Impact Makers does not have 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 **[X]** NO

IF YES, EXPLAIN:

VI. Small Business Subcontracting Plan

ATTACHMENT B

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

Offeror Name: Impact Makers, Inc. **Preparer Name: Impact Makers, Inc.**

Date: 1/30/25

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No __X___

If yes, certification number: _____NA_____ Certification date: _____NA_____

Is your firm a **Woman-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 **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_____ No__**X**__ 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).

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: RFP# FDC-1220 JMU IT Security Auditing Services
Date Form Completed: 1/27/25

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

Offeror / Proposer:
Impact Makers (Firm) 3200 Rockbridge Street, Suite 200, Richmond, VA 23230 (Address)
Contact Person/No. Joe Pugh (804) 641-1551

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)
Rattlesnake Creek LLC 4635 Arrowhead Road Richmond, VA 23235	Scott Hammer (804) 306-9685	830321	IT Security Audit and Assessment Services	20% of work contracted	

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

VII. Sales to VASCUPP Members

The below section is meant to identify the amount of sales Impact Makers had during the last twelve months with each to address the requirement in Section V, Paragraph B, Item #6.

VASCUPP Member	Sales in last 12 months
George Mason University	$400,000
James Madison University	$ 25,000
Norfolk State University	$77,900
Richard Bland College of the College of William and Mary	$70,880
Virginia Community College System[1]	$109,500

VIII. Proposed Cost / Rate Card

The below section is the proposed costs, including an hourly rate breakdown by position type for the proposed services to address the requirement in Section V, Paragraph B, Item #6 and Section X.

For each engagement, Impact Makers will determine the level and amount of staffing needed to meet the University's requirements. Additionally, Impact Makers will coordinate with the project's management in order to determine the amount of time required to be on-site in order to meet the requirements for each assessment. The rates are **not to exceed** the amounts depicted below; Impact Makers has generally provided services under its existing contract at rates significantly lower than this rate card. In particular, Impact Makers will endeavor to minimize the travel expense charged to the University by scheduling on-site work as effectively and efficiently as practicable. Please note that these are the same rates as Impact Makers' current rates through our contract pursuant to JMU RFP# FDC-1057; we have not increased these rates from the current contract.

Tier	Hourly Rate (On-Site)	Hourly Rate (Off-Site)
Associate Consultant	$ 127.18	$ 105.98
Consultant	$ 169.57	$ 148.38
Senior Consultant	$ 190.77	$ 169.57
Lead Consultant	$ 211.97	$ 190.77
Principal Consultant	$ 233.16	$ 211.97

[1] While the Virginia Community College System is not a VASCUPP member, the services Impact Makers provided to it were provided through Impact Makers' contract pursuant to JMU RFP# FDC-1057.

IX. About Impact Makers

Impact Makers understands the importance to JMU of the services requested in RFP# FDC-1220. We believe that we can best support JMU's IT security assessment and audit needs because of our:

- Exceptionally seasoned, senior consultants who have **deep risk management and IT risk assessment and IT security audit experience** (see Resumes and Qualifications, above).
- **Extensive experience** in conducting IT risk assessments and IT security audits for JMU and other Commonwealth of Virginia (COV) institutions of higher education and agencies.
- Specific familiarity with industry-standard security and risk management planning because **our consultants developed security programs and plans** for multiple COV agencies and for institutions of higher education.
- Related **risk management and IT security support** experience.
- **Very satisfied clients** who trust their most important projects to us and attribute the success of their organizations to our business and related consulting support (see Project Qualifications & Reference above).
- A compelling business model – Impact Makers is committed to **contributing our profits and pro bono consulting to charities** in the Richmond area.

We are a Richmond, Virginia-based management and technology consulting company. Started in 2006 as one of the first Benefit Corporations in Virginia, we operate as a for profit company with a social mission to help local non-profits through our pro bono work and financial contributions. Impact Makers has provided over $4.7 million in direct financial support to non-profit community partners as well as over 11,000 pro bono hours of our consultants' management and technical consulting expertise.

Impact Makers has been a leading provider of management and technology solutions to a variety of clients since our founding over 18 years ago. IT risk assessments and IT security audits are among our core services, and we have also provided these services to a variety of clients.

We also believe that our community-focus and our profits to charity model aligns well with JMU and its mission. We believe that our expertise and experience, our approach, our expert team, our qualifications, and our unique business model and mission will combine to make this proposal compelling to you. We hope you will agree and look forward to the opportunity to work with you. We are also happy to provide any additional information you may require.

Impact Makers is a for profit management and technology consulting firm that is committed to contributing 100% of its net profits to the community over the life of the company. Our community contributions rival those of companies a hundred times our size due to this revolutionary model. As a founding B Corp, we have been named "Best for World" and have ranked on the Inc 5000 Fastest Growing Companies numerous times.

What Makes Impact Makers Unique?

At Impact Makers, we are redefining business. Our passion is doing the right thing to create meaningful change for our clients and our community. We drive change through our teams of exceptional people, motivated by our mission and guided by our values. Achieving success is a different experience with us, by design.

Impact Makers is committed to contributing our profits and equity to the community. Our financial and professional support contributes significantly to the ability of nonprofit community partners to empower and support tens of thousands of citizens in our communities. Our community partners include:

- **Family Lifeline** helps families succeed & assists Central Virginia's most vulnerable children, parents & seniors by providing support, wellness & education.
- **Rx Partnership** provides free prescription medications to qualifying uninsured patients of Virginia's free clinics.
- **IT 4 Causes** provides stable, secure & sustainable information technology solutions that enable other non-profit organizations to focus on their missions and serve their clients better.
- **The Podium Foundation** offers student writing workshops to Richmond youth, encouraging creative expression while developing essential writing & communication skills.

- **The Virginia Association of Free and Charitable Clinics** advocates for the issues and concerns of free and charitable clinics, their volunteer workforce of health care professionals, and the patients served by free and charitable clinics in communities throughout the Commonwealth.
- **Samaritan House** has provided emergency and permanent housing, support services and community outreach to victims of violence and homeless families in the Hampton Roads region since 1984.
- **KLM Scholarship Foundation** provides scholarship awards to academic-based and target college students faced with financial obstacles.
- **Tech For Troops** empowers the under-resourced Veterans, Active Duty and their families by providing mental wellness triage and sustainable lifelong digital skills backed through training, education, and technology.

The figure below depicts our business model and its impact, as demonstrated by the impact our support has had on our community partners.

Figure 2 – Impact Makers' Business Model and Values

Clients that engage Impact Makers not only achieve their business goals via the work of Impact Makers' team of experienced consultants, but also contribute directly to the welfare of the community through Impact Makers' donation of profits to our community partners. The figure below depicts how Impact Makers' business model benefits our clients, non-profit partners, and the community.

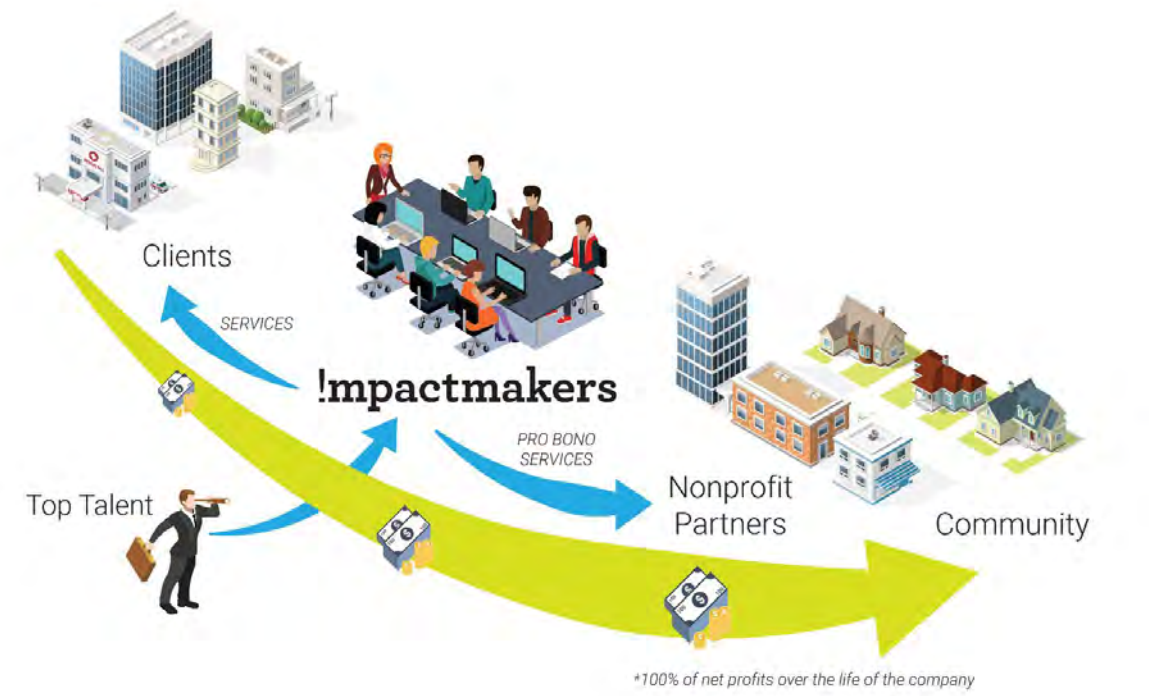

Figure 3 – Impact Makers Serves Clients, Partners, and the Community

X. Appendix – Yellow Book QAR Review Letter

Richard H. Tarr, CIA, CISA

November 15, 2022

Tim Lindsay
Enterprise Portfolio Director
Impact Makers
3200 Rockbridge St, Suite 201
Richmond, VA 23230

Dear Mr. Lindsay,

I have completed a peer review of the internal audit activity at Impact Makers for the period August 2, 2021, through August 22, 2022. Following Government Auditing Standards (Yellow Book standards) peer review requirements, I followed the standards and guidelines contained in the Peer Review Guide published by the Association of Local Government Auditors (ALGA)

I reviewed the internal quality control system of your audit organization and conducted tests to determine whether your internal quality control system was adequately designed effectively to provide reasonable assurance of compliance with the Yellow Book standards issued by the Comptroller General of the United States and applicable legal and regulatory requirements. My procedures included:

- Reviewing your audit organization's Description of the Quality Control System.
- Reviewing your audit organization's Policies and Procedures Manual.
- Reviewing documents related to independence, experience, training, and development of audit staff.
- Interviewing a sample of audit staff members to assess their understanding of, and compliance with, relevant quality control policies and procedures.

Due to variances in individual performance and judgment, compliance does not imply adherence to standards in every case but does imply adherence in most situations. Organizations can receive a rating of pass, pass with deficiencies, or fail. Impact Makers has received a rating of **pass.**

This rating is based on there being in place the structures, policies, and procedures necessary to conduct an audit following the Yellow Book standards. However, the operating effectiveness of these structures could not be evaluated because to date no client has requested an audit project that conforms to the Yellow Book standards.

Further, based on the results of my review, it is my opinion that Impact Makers' internal quality control system is adequately designed to provide reasonable assurance of compliance with the Yellow Book standards and applicable legal and regulatory requirements for performance audits and non-audit services.

Richard H Tarr, CIA, CISA

PO Box 560716 **Orlando, FL 32856-0716** **407.896.2760** **rtarr@racar.com**

JAMES MADISON UNIVERSITY

Request for Proposal

RFP# FDC-1220

Information Technology Security Auditing Services

December 17, 2024

James Madison University will be closed from December 20, 2024 – January 1, 2025

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

ANSWER/INQUIRY SUBMISSION FORM

DEADLINE FOR SUBMISSION OF QUESTIONS: Wednesday, January 8, 2025 @ 5:00 p.m.

****PROCEDURE FOR SUBMITTING QUESTIONS****

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, and Item number within the Statement of Needs specifications of this document that the question is in reference to.

Questions shall be submitted to Doug Chester at the following e-mail address: chestefd@jmu.edu.

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.

Date: _____

Project Location: James Madison University
Project # & Title: FDC-1220 Information Technology Security Auditing Services

The following question concerns: (indicate)

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

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Question submitted by:

_____

Name Organization E-mail Address

REQUEST FOR PROPOSAL
RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

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

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

Sealed Proposals Will Be Received Until 2:00 PM on January 21, 2025 for Furnishing The Services Described Herein. (See Special Terms & Conditions "D. Late Proposals")

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

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

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

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature)

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:
ÿ YES; ÿ NO; ***IF YES*** ⇒⇒ ÿ SMALL; ÿ WOMAN; ÿ MINORITY ***IF MINORITY***: ÿ AA; ÿ HA; ÿ AsA; ÿ NW; ÿ 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-1220

TABLE OF CONTENTS

I. PURPOSE

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

II. BACKGROUND

James Madison University (JMU) is a comprehensive public institution in Harrisonburg, Virginia with an enrollment of approximately 22,000 students and approximately 4,000 faculty and staff. There are over 600 individual departments on campus that support seven (7) academic divisions. The University offers over 120 majors, minors, and concentrations. Further information about the University can be found at the following website: www.jmu.edu.

The mission of James Madison University's Audit and Management Services (AMS) is to assist the university's management and the JMU Board of Visitors by providing independent, objective assurance and consulting services designed to add value and improve university operations.

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

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

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

IV. STATEMENT OF NEEDS

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

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

C. The University's AMS requires, at a minimum, the following supplemental support for its IT auditing functions:

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

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

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

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

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

D. Billing Rate:

The Offeror shall provide an off-site hourly rate broken down by position type for the proposed services and a flat fee onsite hourly rate that includes all billables (e.g., travel, lodging, etc.). Pricing for all other products and services shall also be included.

E. Additional Information

1. The number of FTEs could vary for each project; however, most projects can be completed by one person if that person has the expertise.

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

3. The contractor will be paid according to the statement of work developed for a given project. If applicable, JMU will issue a 1099 to the contractor for the amount paid in the calendar year.

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

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

6. JMU follows ISO 27002 for security framework guidance and networking equipment compliance, along with industry-standard best practices.

7. The overall contract may be awarded to multiple companies as needed to ensure that JMU has the expertise to support our audit plan. Each project will then be contracted separately with a selected contractor. A pre-audit conference is conducted to develop the scope of work for each project. The contractor then submits a proposal for the project with an estimate of the project's hours (and total cost). Approval of the proposal by AMS and the issuance of a purchase order to authorize the work create the contract for the project.

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

   Depending upon the project, the work may be done entirely off-site or require on-site testing with off-site report writing and follow-up.

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.

ELECTRONIC OR PAPER SUBMISSIONS MAY BE ACCEPTED FOR THIS PROPOSAL. INSTRUCTIONS BELOW FOR OFFEROR'S CHOSEN METHOD (A. ELECTRONIC SUBMISSION or B. PAPER RESPONSE).

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. **ELECTRONIC SUBMISSION**:

      i. ELECTRONIC RESPONSES SUBMITTED THROUGH eVA WILL BE ACCEPTED. **Emailed responses will not be accepted.** Please see below, "eVA Procurement Website and Registration" for additional information on registration. It is the responsibility of the Supplier to ensure their proposal and all required documentation is properly completed, readable, and uploaded to eVA. Suppliers should allow sufficient time to account for any technical difficulties they may encounter during online submission or uploading of the documents. In the event of any technical difficulties, Suppliers shall contact the eVA Customer Care Center at 1-866-289-7367 or via email at eVACustomerCare@DGS.virginia.gov.

      ii. eVA Procurement Website and Registration The Commonwealth's procurement portal, eVA, located at http://www.eva.virginia.gov, provides information about Commonwealth solicitations and awards. Suppliers shall be registered in eVA in order submit a proposal to this

RFP. To register with eVA, select "Register Now" on the eVA website homepage, http://www.eva.virginia.gov. For registration instructions and assistance, as well as instructions on how to submit proposals and accept orders please select "I Sell to Virginia". Suppliers are encouraged to check this site on a regular basis and, in particular, prior to submission of proposals to identify any amendments to the RFP that may have been issued.

iii. Electronic Responses submitted through eVA shall be in WORD format or searchable PDF of the entire proposal, INCLUDING ALL ATTACHMENTS. PDFs must be submitted in an unlocked format. Any proprietary information should be clearly marked in accordance with Section V.4.e below.

b. **PAPER SUBMISSIONS:**

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

ii. **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.

iii. 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.

iv. See additional information in Section VIII.C, *IDENIFICATION OF PROPSAL ENVELOPE*.

2. Should the proposal contain **proprietary information**, **provide one (1) redacted 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.

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

4. Proposal Preparation

   a. Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in the purchasing agency requiring prompt submissions of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

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

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

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

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

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

5. 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. (Electronic signature shall be accepted, i.e. Adobe Sign, DocuSign, etc.)

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

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

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

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

6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org.
7. Proposed Cost. See Section X. Pricing Schedule of this Request for Proposal.

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

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

		Points
1.	Quality of products/services offered and suitability for intended purposes	25
2.	Qualifications and experience of Offeror in providing the goods/services	25
3.	Specific plans or methodology to be used to perform the services	20
4.	Participation of Small, Women-Owned, & Minority (SWaM) Businesses	10
5.	Cost	20
		100

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

VII. GENERAL TERMS AND CONDITIONS

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

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

C. ANTI-DISCRIMINATION: By submitting their proposals, offerors certify to the Commonwealth that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and §10 of the Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 (available for review at http://www.jmu.edu/procurement). If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender, 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. PRECENDENCE OF TERMS: Paragraphs A through J of these General Terms and Conditions and the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors, shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

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

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

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

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

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

2. The Purchasing Agency may order changes within the general scope of the contract at any time by written notice to the contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The contractor shall comply with the notice upon receipt. The contractor shall be compensated for any

additional costs incurred as the result of such order and shall give the Purchasing Agency a credit for any savings. Said compensation shall be determined by one of the following methods:

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

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

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

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

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

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

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

2. Employer's Liability: $100,000

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

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

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

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

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

T. NONDISCRIMINATION OF CONTRACTORS: An offeror, or contractor shall not be discriminated against in the solicitation or award of this contract because of race, religion, color, sex, 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 nonresponsive 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 via email directly to the Procurement Officer listed on the signature page of this solicitation or 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 or swamreporting@jmu.edu .**

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 or swamreporting@jmu.edu** . 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 or swamreporting@jmu.edu** .

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

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

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

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

IX. METHOD OF PAYMENT

The contractor will be paid 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 an off-site hourly rate broken down by position type for the proposed services and a flat fee onsite hourly rate that includes all billables (e.g., travel, lodging, etc.). Pricing for all other products and services shall also be included. The resulting contract will be cooperative, and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2.

Specify any associated charge card processing fees, if applicable, to be billed to the university.

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

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

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

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

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

   Years_____ Months_____

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

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

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

ATTACHMENT B

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

Offeror Name: _____ Preparer Name: _____

Date: _____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date: _____

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: _____ Date Form Completed:_____

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

Offeror / Proposer:

_____	_____	_____
Firm	Address	Contact Person/No.

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

(Form shall be submitted with proposal and if awarded, a SWaM Sub-contractor Reporting Form shall be submitted to swamreporting@jmu.edu)

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

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

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

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

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

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

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

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

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

ATTACHMENT D

Zone Map

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

List of member institutions by zones

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

JAMES MADISON UNIVERSITY

January 10, 2025

ADDENDUM NO.: One

TO ALL OFFERORS

REFERENCE:	Request for Proposal No:	RFP# FDC-1220
	Dated:	December 17, 2024
	Commodity:	Information Technology Security Auditing Services
	RFP Closing On:	~~January 21, 2025 at 2:00 p.m.~~
		January 30, 2025 @ 2:00 p.m.

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

Due to the number of questions received for this RFP, James Madison University has extended the closing date to **January 30, 2025, at 2:00 p.m**.

A second addendum will be posted next week with responses to vendor questions.

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

January 16, 2025

ADDENDUM NO.: Two

TO ALL OFFERORS

REFERENCE:	Request for Proposal No:	RFP# FDC-1220
	Dated:	December 17, 2024
	Commodity:	IT Security Auditing Services
	RFP Closing On:	January 30, 2025 @ 2:00 p.m.

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

AMS refers to JMU's Office of Audit Management Services

The following questions are answered below:

1. Are the audits listed in a. through j. all intended to be completed in the one-year contract?

   Answer: The audits listed are a population of potential audits. Typically, 3-5 are selected each year.

2. Has the University contracted with outside service providers to conduct IT Security Audits in the past? If so:
   a. When were the most recent IT Security Audits conducted and what was the scope?
   b. Who was the service provider?

   Answer: Yes. We typically have 3-5 done annually by our contracted vendors.

3. Would the University be willing to share the results of prior IT Security Audits with the awarded vendors?

   Answer: Results are FOIA exempt. They could potentially contain sensitive security information and will not be shared.

4. Does the University have a preference for awarding this project to service providers who have conducted work within the Commonwealth of Virginia?

   Answer: The vendor must be registered to work within the Commonwealth of Virginia and with eVA (https://eva.virginia.gov).

5. Does the University's AMS intend to provide resources and staff to support the IT Security Audits, or is the vendor to provide all the resources?

   Answer: The IT Auditor in AMS manages the audits, assists consultants during the audit, arranges the entrance conference for each audit, and ensures consultants have what they need to complete the audit (credentials, etc.).

6. Will the requested IT Security Audits be required to be conducted to meet Institute of Internal Auditors (IIA) standards?

   Answer: Not required

7. Will the requested IT Security Audits be considered performance audits under Yellow Book?

Answer: No

8. What is the requested start and completion date of the one-year contract?

   Answer: The contract will start after the successful completion of the RPF process. The contract will last for one year and have four optional one-year renewals.

9. Does the University use an audit tracking or compliance software that the audit results will be imported into? If so, what?

   Answer: Documents related to each audit are stored in AMS automated workpaper system.

10. Does the University have an allocated budget for this engagement that can be shared with proposers?

    Answer: AMS has a fixed budget for IT Security Auditing projects.

11. The RFP states, "The selected contractor(s) shall supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit." This seems to indicate that all work will be performed in a staff aug capacity to where JMU leadership will supervise all of the winning bidder's team instead of the bidder's Partner/ Principal/Director's leadership. Can you confirm if this is accurate or if some audits will be co-sourced entirely to the bidder such that the bidder's leadership team is responsible for staff supervision and review of the final deliverables.

    Answer: The contractor chosen to conduct an audit will manage their own staff. AMS will provide assistance to ensure that they have what they need to complete the audit. See #5 answer

12. Does JMU have any estimate for what percentage of the audits or work hours will need to be performed onsite vs just done remotely?

    Answer: Onsite or remotely depends on the audit. Most are done remotely.

13. Does JMU have a planned annual budget for these services or some idea of how many audits will need to be staffed with the winning bidder?

    Answer: AMS has a fixed budget for IT Security Auditing projects. AMS meets with IT annually to discuss the year's upcoming IT audits. Cost is one of the factors that determine the number of audits.

14. Can you clarify if SWAM participation is required or optional, and how will the 10 pts for SWAM usage be scored?

    Answer: SWaM participation is not required. However, JMU strives to work with SWaM vendors whenever practicable. A SWaM vendor would get 10 points if they are a certified SWaM vendor (registered with the Virginia Department of Small Business and Supplier Development (VSBSD)). A non-SWaM vendor utilizing SWaM sub-contractor (registered with VSBSD) would receive some portion of the 10 points available.

15. Can you clarify whether the projects require a mix of on-site and off-site work, or are they predominantly one or the other?

    Answer: Audits are typically either on-site or remote and determined during planning.

16. How will the scope of work for each project be defined? Will templates or prior examples be provided?

    Answer: The scope of audits are typically defined during an entrance conference meeting.

17. What are JMU's highest-priority areas for IT security auditing? Are there any recent audit findings that should be addressed in these engagements?

    Answer: AMS conducts a risk assessment annually. In the past, audits have been on a three-year cycle. Systems that support critical functions are considered a higher priority to assess.

18. Will JMU require resumes or bios for assigned staff during each project proposal?

    Answer: Bios for staff are required for the initial review and selection process. We will select 3-5 organizations to have on contract.

19. Are subcontractors allowed, and if so, are there any restrictions or additional requirements?

    Answer: Yes, they are allowed. Organizations may need to provide bios for any subcontractors used prior to any audit.

20. Can you elaborate on the specific deliverables required for each type of audit (e.g., penetration testing, vulnerability scans, etc.)?

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

21. Are sample reports or templates available for review?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

22. What specific systems, applications, or networks are in scope for the penetration testing? Are there any excluded systems, applications, or segments of the network?

    Answer: All of our systems are potential candidates for audits. What will be included in an audit will be determined during an entrance conference.

23. What are the primary objectives of the penetration testing (e.g., vulnerability identification, exploit validation, compliance verification)? Is the focus on internal, external, or hybrid penetration testing?

    Answer: Pen tests will be conducted from both internal and external perspectives. The objectives are determined during an entrance conference.

24. Does JMU have a preferred penetration testing methodology (e.g., OWASP Testing Guide, PTES, or NIST SP 800-115)?

    Answer: We do not have a preferred methodology as long as the methodology used is well known.

25. Are automated scanning tools allowed, or is manual testing preferred?

    Answer: Yes, automated scanning tools are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

26. How often does JMU require penetration testing to be performed (e.g., annually, quarterly)?

    Answer: Annually for GLBA requirement. Network is every other year. Systems that support critical functions once every three years (hosted systems).

27. Will ad-hoc testing be required for major system changes or incidents?

    Answer: In the past, IT has used our contract to have a consultant assess a system after an upgrade.

28. Can JMU provide a network diagram, including segmentation and firewall configurations, to help define testing boundaries?

    Answer: Yes, if necessary, these will be provided prior to an audit.

29. Are there any cloud-based services or hybrid infrastructure elements that need to be tested?

    Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

30. Will test accounts with specific privileges (e.g., admin, standard user) be provided for application testing?

    Answer: Yes, the appropriate accounts will be provided to consultants to complete an audit.

31. Is testing expected to include credentialed scans or only external unauthenticated testing?

    Answer: This will depend on the scope of the audit, which will be determined during an entrance conference.

32. Are wireless networks within scope? If so, how many wireless networks exist, and are separate SSIDs used for guest and internal networks?

    Answer: A wireless network audit is a potential engagement. Actual numbers and SSIDs will be discussed during planning.

33. Are there compliance frameworks or regulatory requirements guiding the penetration testing (e.g., NIST 800-53, ISO 27001, FERPA, HIPAA)?

    Answer: This would be discussed in planning for each project. It could depend on the type of data being processed/stored in the target area.

34. Are there specific reporting formats or templates required to align with these standards?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

35. Are there restrictions on the tools, scripts, or software that can be used during testing?

    Answer: No, all automated scanning tools, scripts and software are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

36. Is social engineering (e.g., phishing or pretexting) included in the scope?

    Answer: Social engineering typically is not included in an audit.

37. Will JMU provide a “blue team” to coordinate defensive responses during testing?

Answer: The Information Security Officer is included in all phases of the audit and will handle defensive responses initially and will delegate to the necessary staff to address.

38. Does JMU expect formal red-team engagements or assume passive observation?

    Answer: Engagements are typically more red team.

39. What specific details are required in the final penetration testing report? (e.g., executive summary, findings by severity, recommendations, risk matrix)

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

40. Should reports include mitigation strategies or just identified vulnerabilities?

    Answer: Recommendations on how to remediate the findings are typically included.

41. Does JMU have a preferred risk rating framework for findings (e.g., CVSS scores, custom classifications)?

    Answer: Consultants are free to use any framework.

42. Are proof-of-concept exploits required to demonstrate identified vulnerabilities?

    Answer: They should be included as supporting evidence for identified issues.

43. Is there a process for safe exploitation to minimize downtime or disruptions?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing.

44. Will follow-up testing be required after remediation efforts?

    Answer: Some audits may require follow-up testing.

45. Should the proposal account for retesting as part of the deliverable or provide optional pricing for retesting?

    Answer: Yes, if it is determined during the entrance conference that follow-up testing will be part of the engagement. Otherwise, follow-up testing will be a separate engagement.

46. Is there a dedicated staging or test environment, or will testing occur in the production environment?

    Answer: This will be determined during an entrance conference. Some core systems do have a test environment.

47. What safeguards need to be followed when testing in production?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

48. Are there restricted testing windows to avoid disruptions to university operations?

Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

49. What are JMU's preferred schedules for conducting tests (e.g., weekends, nights)?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

50. What is the process for notifying stakeholders and getting approvals prior to testing?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

51. Are there specific points of contact required during the testing period?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

52. Are there data privacy or legal restrictions that must be observed during testing (e.g.,FERPA, HIPAA)?

    Answer: The university must comply with many regulations, including, but not limited to, HIPAA, FERPA, and GLBA. Consultants are required to proceed cautiously with testing to ensure the security of university systems and data.

53. Will there be specific contract terms to limit liability for findings related to downtime or data exposure?

    Answer: AMS is not sure how a finding could create liability.

54. Are NDAs required for testers, and if so, will templates be provided?

    Answer: Yes, NDA's may be required. A template will be provided.

55. What is JMU's process for responding to vulnerabilities or breaches identified during testing?

    Answer: In most cases, university staff will contact the vendor of the system to determine a resolution.

56. Will testers be involved in drafting incident response plans or conducting tabletop exercises?

    Answer: This has not been done in the past.

57. Does JMU expect named resources (e.g., resumes, certifications) to be identified in the proposal?

    Answer: It would be helpful to identify all potential staff and their experience. This will help us to select the most qualified consultants to have on contract.

58. Is there a minimum certification level required (e.g., OSCP, CEH, GPEN)?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

59. Should pricing account for fixed-price engagements, or does JMU prefer time and materials pricing for penetration testing?

    Answer: Consultants should provide an hourly rate for on-site (inclusive of travel) and an hourly rate for remote/off-site work.

60. Are there restrictions on billing categories, such as separate charges for travel and software licenses?

    Answer: Allowable expenses will be discussed during planning.

61. Does JMU require post-engagement workshops or training sessions for internal IT staff?

    Answer: If there are findings, all that is needed are recommendations and appropriate resolutions.

62. Should documentation include step-by-step remediation guidance for IT teams?

    Answer: Any information that will help resolve a finding should be included in a recommendation.

63. Is ongoing vulnerability scanning or maintenance required as part of the contract?

    Answer: The engagements will be a point-in-time assessment of systems.

64. Should pricing for managed services or recurring assessments be included?

    Answer: The engagements will be a point-in-time assessment of systems.

65. Will JMU provide access to any tools, software, or scanning platforms?

    Answer: This has not been done in the past. Consultants have been required to use their own tools.

66. Are there restrictions on third-party tools we can use?

    Answer: The university expects that consultants will use reputable tools during engagements. Any questions about tools can be discussed during planning.

67. How frequently are status reports or updates required?

    Answer: Not all engagements are the same and this will be discussed during planning.

68. Are there any formal review or sign-off processes for deliverables?

    Answer: AMS has an internal review and sign-off process for deliverables received during the engagement.

69. Does JMU prefer fixed-price or time-and-material pricing structures for specific projects?

Answer: Consultants should provide an hourly rate for on-site (including travel) and an hourly rate for remote/off-site work.

70. Should travel costs be itemized separately or included in flat rates?

    Answer: Included in flat rates.

71. What invoicing formats and documentation are required for payment processing?

    Answer: There is no requirement for a specific format. An invoice with the costs associated with completing the engagement should be submitted for payment.

72. Are there specific payment terms for milestone-based deliverables?

    Answer: Payment for engagements is handled when the final report is provided to AMS. There are no exceptions to this.

73. What are the requirements for on-site visits, including badging and access controls?

    Answer: This will be discussed during planning. Typically, consultants are provided with credentials for testing. They will be escorted through sensitive areas if required.

74. Are there specific blackout dates or periods where testing cannot occur due to academic schedules?

    Answer: Yes. Typically, testing will be conducted during times to minimize any impacts.

75. Would the University consider accepting certifications other than those listed in the definition of "Certified Professional" on p. 2 (for example, ITIL Foundation v3, Certified Associate Chief Information Security Officer (C | CISO)? Also, could you please clarify whether all team members must fit the definition of Certified Professional, or if it's sufficient that each engagement be led by consultants with the required certifications?

    Answer: Yes, alternate certifications could be acceptable. Not all team members would need certifications, as long as they are under supervision of a certified consultant.

76. Are there any GLBA or PCIS audit needs that should be included?

    Answer: GLBA required audit is a potential engagement.

77. Is there a preference for NIST 800 or ISO 27001 compliance frameworks?

    Answer: Currently, JMU IT is using ISO.

78. Does this count as a VASCUPP award or is this just for JMU?

    Answer: This contract will be made available to the VASCUPP schools for their use, should they choose to do so. This will be a cooperative contract that can be utilized by 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

79. When is the next anticipated need for audit work to start at JMU?

    Answer: The goal is to have the selected consultants on contract before the end of the current fiscal year. Most likely, the need will not be until next fiscal year (7/1/2025-6/30/2026).

80. The RFP states "Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP)." This Reads as if all of the listed certifications are required for each consultant. Is that correct or is it just that a consultant must have one of the listed certifications for their appropriate area to be deemed a certified professional?

    Answer: At least one of the certifications.

81. Can you explain the last two columns of the table in Attachment B, specifically:
    "Total Subcontractor Contract Amount"
    "Total Dollars Paid Subcontractor to date"

    Answer:

    Total Subcontractor Contract Amount – Dollar amount allocated to SWaM subcontractor in the direct performance of the contract/task.

    Total Dollars Paid Subcontractor to date – The total dollar amount paid by the contract to the subcontractor.

82. Do the columns refer to work previously performed where the Offeror has used the sub-contractor to perform work? Does either value represent an estimate of what work might be performed by a given contractor?

    Answer: No. They should represent an estimate of the what work might be specific to the contract.

83. Under section 5 Part B #6, the ask is to identify sales in the past 12 months to VASCUPP members. Many of these institutions have moved to the VHEPC contract. Can VHEPC data be used in the response?

    Answer: Yes

84. Could you kindly provide information regarding the current budget allocated for these services or details about the prices paid under previous contracts for similar services?

    Answer: Our current budget has been sufficient to do GLBA testing and two to five other projects each year. Each project is carefully planned and scoped with input from JMU's IT and the consultant.

85. Will the University be permitting penetration testing to be performed by existing or previous IT or Managed Service Providers? Or will the University be requiring third-party independence to reduce the risks of conflicts of interest or the optics of "grading one's work"?

    Answer: We are looking to have contracts with some consultants who will perform pen tests.

86. Is the University currently using any service providers that are assisting the University in performing the requested services? If so, who are these providers?

Answer: The current providers can be found here.

87. Is there an incumbent providing similar services to the University? If yes, is the incumbent performing to the satisfaction of the University, and the Chief Information Security Officer?

    Answer: See the answer to question 86 above.

88. Is the incumbent eligible to bid on this contract?

    Answer: Yes.

89. Can the University provide any information on the budget required to support these services? (E.g., budget details)

    Answer: AMS has a fixed budget for these services and cost will be a factor. No more details about the budget will be provided.

90. Does the University have onsite audit preference or vendor can perform remotely?

    Answer: Potential engagements include on-site. There is no preference.

91. Can the University provide a brief high-level description and accounting of their computing infrastructure? (e.g., hard-wired versus wireless, Windows and or Linux and or Mac, number of domains, number networks, number of IP addresses, etc.)

    Answer: If necessary, infrastructure will be discussed during planning for each engagement.

92. How many of the external IP addresses are live or currently in use?

    Answer: Will be discussed during planning for each engagement if necessary.

93. For wireless access points, how many SSIDs and how many locations are in scope?

    Answer: Will be discussed during planning for each engagement if necessary.

94. Are all campus/network locations accessible from the central location of the network?

    Answer: Will be discussed during planning for each engagement if necessary.

95. Is there a EDR solution is in place? If so, what vendor is it? Is it centrally managed?

    Answer: The university refrains from answering this question.

96. Is there a cybersecurity department? Is there an ISO or CISO on staff?

    Answer: The university has an ISO. University IT manages cybersecurity.

97. When was the last time an overarching IT security risk assessment was performed?

    Answer: JMU conducts various risk assessments to meet the needs of the University.

98. Does the University have documentation of the designated system owners and data owners?

    Answer: Yes

99. Is there a conclusive/documented inventory of all assets in scope that can be provided to selected Vendor?

Answer: Will be discussed during planning for each engagement.

100. Does the University currently utilize any internal network vulnerability assessment tools? If so, what is the scan frequency?

Answer: Yes. The university refrains from answering this question.

101. Does the University use baseline images for systems?

Answer: Yes

102. Is formalized change management in place?

Answer: Yes

103. How many voice VLANS and IP phones are in-scope?

Answer: Will be discussed during planning if necessary.

104. How many wireless locations are in-scope?

Answer: Will be discussed during planning if necessary.

105. Does the University want any cloud environments tested? If so, which vendor?

Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

106. Does the University have any remote access services in use (on-demand VPN, GoTo my PC, LogMeIn, etc.) in-scope?

Answer: Will be discussed during planning if necessary.

107. Does the University have any in-bound modems (or remote access) in use?

Answer: Will be discussed during planning if necessary.

108. Is there any allowability to redline terms and conditions to negotiate later?

Answer: Will be discussed during planning if necessary.

109. The RFP is titled “Information Technology Security Auditing Services”, will all projects awarded be strictly security focused? For instance, the statement of needs mentions wireless network assessment/server configuration which can include many considerations aside from security.

Answer: Engagements will be focused on security to assess the controls protecting university systems and data.

110. How is the security team currently staffed/structured and how would you describe your current approach to security?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

111. Is there a routine and scheduled IT and Security audit services?

Answer: AMS works with IT annually to create the annual audit plan.

112. How often does JMU conduct IT and Security Audit assessments?

Answer: Up to five consultant engagements may be conducted during a fiscal year.

113. Who manages the IT and Security Audit service schedules for JMU?

Answer: Most are managed by the IT Audit Specialist in AMS.

114. Is each academic division responsible for managing its own IT asset?

Answer: Some academic units manage their own systems.

115. Is each academic division responsible for conducting routine and scheduled IT and Security Audit?

Answer: They are included in audits managed by AMS

116. Who is Audit and Management Services (AMS)? Is this an external entity, like a contractor hired by JMU to perform routine IT And Security Audit services? Or, is AMS a division within JMU?

Answer: AMS is JMU's internal audit department.

117. Who is responsible for managing JMU's IT Assets?

Answer: Central IT manages most IT assets.

118. Does JMU keep an inventory list of its IT Assets?

Answer: Yes

119. Who tracks JMU's IT Assets?

Answer: Central IT manages most IT assets.

120. Does each academic division track its own IT Assets?

Answer: Yes

121. Who performs routine and scheduled maintenance?

Answer: Central IT for most systems

122. Is this RFP to replace the existing/current staff of contractors performing under formal Statement of Work agreement?

Answer: The current contracts expire in April of 2025.

123. Is this RFP to provide supplemental support to JMU Personnel performing IT Audit functions listed in Section IV, Paragraph C (a-j)?

Answer: Yes, we outsource highly technical audits, such as pen tests and vulnerability assessments. JMU's IT Auditor oversees the outsourced projects.

124. Is this RFP to also provide supplemental support to current Staff of Contractors that are performing IT Audit functions under formal Statement of Work agreement?

Answer: This RFP is to support JMU's AMS department.

125. How many Staff of Contractors currently provide IT Audit Services to JMU-AMS under formal Statement of Work agreement?

Answer: We have four vendors on contract.

126. How many of these IT Audit functions are being performed by JMU Personnel?

Answer: The listed examples are performed by consultants.

127. How many of these IT Audit functions are being performed by the Staff of Contractors that are performing under formal Statement of Work agreement?

Answer: The listed examples are performed by consultants.

128. How many web applications are being assessed?

Answer: This will be determined during planning.

129. What framework and platform are being used for the web application(s)?

Answer: This will be discussed during planning.

130. How many static pages are being assessed? (approximate)

Answer: This will be discussed during planning.

131. How many dynamic pages are being assessed? (approximate)

Answer: This will be discussed during planning.

132. Will the source code be made readily available?

Answer: No

133. Do you want role-based testing performed against this application?

Answer: This will be discussed during planning.

134. Do you want credentialed scans/assessments of the web applications performed?

Answer: This will be discussed during planning.

135. How many total IP addresses are being tested?

Answer: This will be discussed during planning.

136. How many internal IP addresses, if applicable?

Answer: This will be discussed during planning.

137. How many external IP addresses, if applicable?

Answer: This will be discussed during planning.

138. Are there any security devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

Answer: This will be discussed during planning.

139. Would the University prefer SWaM agencies?

Answer: JMU strives to work with SWaM vendor whenever practicable.

140. Is subcontracting mandatory for SWaM-certified agencies?

Answer: No

141. Would the university award 10 points as per the evaluation criteria to a Prime -SWaM certified agency if the Prime vendor does not subcontract for this opportunity?

Answer: Yes, as long as they are SWaM certified with the VSBSD.

142. How many individual projects or separate Statement of Works were issued under this award in the previous five-year contract period?

Answer: We typically have 3-5 engagements per fiscal year.

143. Can you please provide the total dollar value of work awarded under this award during the previous five-year contract period?

Answer: This information is not readily available.

144. Who is the individual the proposal will be addressed to?

Answer: Instructions are on page 17 of the RFP.

145. The RFP states that a certified professional is defined as someone holding a current CISA, CISSP, CISM, MCP, CCNA, or ISSMP certification. Would JMU consider adding the CompTIA Advanced Security Practitioner (CASP+) to the list? This certification requires 10 years' of hands-on IT experience and at least 5 years of hands-on IT security experience. The certification demonstrates advanced competency in areas such as risk management, enterprise security, and governance.

Answer: This list is not comprehensive. All reputable certifications should be mentioned.

146. Who is responsible for determining the on-site versus off-site requirements?

Answer: This will be discussed during planning.

147. What is the anticipated level of on-site engagement, if any? And how many locations will require an on-site visit?

Answer: This will be discussed during planning.

148. Are there specific workshare requirements under the Small Business Subcontracting Plan?

Answer: There are no requirements to utilize SWaM vendors. However, JMU strives to work with SWaM vendors whenever practicable.

149. Is strict adherence to ISO 27002 security framework requirements mandatory, or are alternative frameworks, such as NIST, acceptable?

Answer: ISO 27002 is preferred. However, any reputable framework could be used.

150. Is it required to provide resumes for all proposed personnel at the time of submission?

Answer: It will help us adequately assess potential consultants if they provide information for all potential staff.

151. Can you confirm the number of wireless networks to be assessed and their respective locations?

Answer: This will be discussed during planning.

152. Could you provide the total number of web applications that require testing?

Answer: This will be discussed during planning.

153. Are there any specific requirements or needs for cloud security assessments in this engagement?

Answer: No. We do not conduct testing on cloud systems.

154. Is the request for a point in time scan of the Universities attack surface or an ongoing service to monitor for external vulnerabilities in real-time?

Answer: The engagements will be a point-in-time assessment of systems.

155. Is there an expectation that active or passive wireless survey would be conducted? If so the locations and floor plans of locations to be surveyed would be needed for an accurate SOW.

Answer: This will be discussed during planning.

156. What are the vendors, models, operating system versions and quantities of firewall and routers in the environment?

Answer: This will be discussed during planning.

157. What server operating system version and number of servers in the environment? Are these servers physical or virtual?

Answer: This will be discussed during planning.

158. What hypervisors are being used in the environment?

Answer: This will be discussed during planning.

159. What IaaS and SaaS platforms are being used in the environment?

Answer: This will be discussed during planning.

160. How many databases are in the environment?

Answer: This will be discussed during planning.

161. What platforms are these databases hosted on?

Answer: This will be discussed during planning.

162. What applications use these databases?

Answer: This will be discussed during planning.

163. Is the intent of this assessment to review the network vulnerability management process?

Answer: This will be discussed during planning.

164. How many web applications are in scope?

Answer: This will be discussed during planning.

165. Where are these web applications hosted?

Answer: This will be discussed during planning.

166. What platforms do these applications run on?

Answer: This will be discussed during planning.

167. What version of Windows are the domain controller running?

Answer: This will be discussed during planning.

168. Is there integration with Entra ID or other identity providers?

Answer: This will be discussed during planning.

169. If the state has already arrived at best market value rates for these services and an contract is in place to reference, why is an RFP being issued?)

Answer: JMU's current contracts for these services will expire in April 2025, and this RFP is being issued to replace them.

170. Is the support requested in the proposal hands-on, or purely advisor in performing an audit of functions conducted by JMU?

Answer: Our goal is to have multiple contractors on contract to provide audit services to assess technical controls. The engagements could be considered hands-on.

171. In order to perform work in this RFP, are contractors required to possess all or some of the certifications listed in Paragraph C? May some of these certifications be alternated pending we have more technical certifications that meet the same requirement?

Answer: It is not required for the staff to possess all the certifications.

172. (C.1.a) Pertaining to conducting External Vulnerability Scanning, are there any third-party assets or assets explicitly excluded from this scope?

Answer: This will be discussed during planning.

173. (C.1.b) Pertaining to conducting Wireless Network Assessments: A) How many networks are in scope? B) How many wi-fi access points are in scope? C) Do we have an up-to-date inventory of all wireless access points (APs) and their locations? D) What is the architecture of the wireless network (e.g., standalone, controller-based, cloud-managed)? E) Are there any mesh networks, IoT devices, or specialized APs in use? F) Are there any known issues with signal interference or channel congestion?

Answer: This will be discussed during planning.

174. (C.1.c) Pertaining to conducting Firewall and Router Security Assessments: A) Does JMU use one specific vendor (ie., Cisco, Juniper, Palo Alto) or a combination of vendors for its solution? If so, which vendors are leveraged within its Firewall and Router solution? B) Are any virtual firewalls or cloud-managed routers part of the assessment? C) Are logs enabled for both firewalls and routers? D) Do you allow telemetry to be exported to external entities (such as our SOC)? E) Are logs integrated with a SIEM (Security Information and Event Management) system for analysis?

Answer: This will be discussed during planning.

175. (C.1.d) Pertaining to conducting Server Configuration Assessments: A) Is there an updated inventory of all servers, including their roles and locations? B) Are server configurations documented and maintained in a central repository? C) Is access to remote management interfaces restricted to specific IPs or networks?

Answer: This will be discussed during planning.

176. (C.1.e) Pertaining to conducting Database Architecture Security Assessments: A) Are both production and non-production environments included in the assessment? B) Is there an updated inventory of all databases, including versions and roles? C) Are database architecture diagrams and data flow diagrams documented and up to date? D) Are logs entralized/monitored (e.g., through a SIEM system)? E) Is there a process for evaluating/applying updates without disrupting operations?

Answer: This will be discussed during planning.

177. (C.1.f) Pertaining to conducting Network Scanning Process Assessments: A) Are the tools configured for active, passive, or hybrid scanning? B) How does the organization discover and inventory all connected devices? C) Are unauthorized or rogue devices detected and flagged during scans? D) What size subnet/subnet range does JMU administer/lease? E) What is an estimate of the number of endpoints to be expected on the network? 500 – 1000, 1000 – 2,500, 2-500 – 5,000, or 5,000+? F) Do you allow telemetry to be exported to external entities (such as our SOC)?

Answer: This will be discussed during planning.

178. (C.1.h) Pertaining to conducting Active Directory Security Assessments: A) How many domains and domain controllers (DCs) are in the environment? B) Are all domain controllers running supported OS versions and fully patched? C) Are logs centralized (e.g., SIEM) and monitored for suspicious activities?

Answer: This will be discussed during planning.

179. (C.1.i) Pertaining to conducting Penetration Testing: A) Are there specific exclusions (e.g., certain servers, critical infrastructure)? B) Is the testing internal, external, or both (e.g., testing from within the network or from an external perspective)? C) Are cloud environments, third-party services, or IoT devices included? D) Is testing white-box (full access), black-box (no prior knowledge), or gray-box (partial knowledge)?

Answer: This will be discussed during planning.

180. (C.1.j) Pertaining to assessing Telecommunications: A) Which telecommunication services are included (e.g., voice, VoIP, wireless, data)? B) Are third-party managed services or service providers within scope? C) Are specific geographical locations or facilities included? D) Are third-party carriers and vendors assessed for security and compliance risks? E) Are contracts regularly reviewed for adherence to terms and emerging security needs? F) Are logs collected, centralized, and analyzed for security events?

Answer: This will be discussed during planning.

181. Please briefly describe what you mean by "Network Scanning Process Assessment" and “Telecommunications”.

Answer: Telecom would focus on the security of the VOIP implementation. The network scanning process assessment has never been included in our audit plan because we feel that we are covered by the internal and external pen tests.

182. Please describe what "other products and services" you typically see in your audits, or what you mean by this phrase.

Answer: We have not had any billing for services other than travel and lodging.

183. What is the typical lead time that you provide to your vendors for your audits?

Answer: During our meeting with IT at the beginning of the fiscal year, we identify the audits to be included for the year as well as identifying the potential consultants. AMS will reach out to those consultants to determine availability and request proposals.

184. Will the universities in each of the listed zones be utilizing services from selected vendors, or just JMU?

Answer: This RFP is being issued for JMU’s needs and will be made available to other VASCUPP schools, should they choose to utilize it. Pricing should be provided so that any VASCUPP school could potentially use it.++

185. How much did JMU spend across all task orders on the previous contract vehicle?

Answer: This information is not readily available.

186. How many task orders were issued on the previous contract vehicle?

Answer: This information is not readily available.

187. What was the work breakdown structure between the 4 incumbents on the previous contract vehicle? Can we see the number of task orders awarded to each contractor?

Answer: This information is not readily available.

188. What is the spending ceiling on the contract vehicle?

Answer: Our current budget is sufficient to support GLBA pen testing, plus 2-5 additional projects per year.

189. Are we required to provide auditing services for all 10 categories, or is it OK to support only a subset?

Answer: No. AMS will contact contractors to submit a proposal for one of the audits when it is on the schedule. It is fine to support a subset of the services.

190. Is certification required for all bidder participants? Can education, training and experience replace certifications?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

191. What brand of firewall equipment are you using?

Answer: This will be discussed during planning.

192. What brand of router equipment are you using?

Answer: This will be discussed during planning.

193. Does your Active Directory (AD) consist of on-premise, Azure AD, or some combination?

Answer: This will be discussed during planning.

194. What types of services does Telecommunications entail?

Answer: This will be discussed during planning.

195. With regards to Telecommunications, what sort of audit or IT activity should be expected? Would this be geared as an audit of process and controls, or a technical assessment for vulnerabilities and penetration testing (i.e. war dialing).

Answer: Telecom would focus on the security of the VOIP implementation.

196. C.1.a - C.1.i- What tools and technologies are currently in place for external vulnerability scanning, network assessments, and penetration testing? Are consultants expected to use university-provided tools or supply their own?

Answer: We expect consultants to use their own tools.

197. Page 3, Paragraph #6: Does JMU provide access to system architecture diagrams, configurations, or previous audit reports to inform the current project scope?

Answer: These will be shared during the planning of an engagement.

198. Page 3, Paragraph A: Since JMU follows ISO 27002, how mature is the current implementation of these controls across IT systems? Are there specific areas of non-compliance that require attention?

Answer: The university refrains from answering this question.

199. C.1.a - C.1.i What level of access will consultants be granted during audits (e.g., administrative privileges, network access)?

Answer: Consultants will be given necessary access to system to complete testing.

200. For on-site engagements, what are the physical security requirements and protocols for accessing sensitive areas of the network or facilities?

Answer: This will be determined during planning of an engagement. Consultants, at a minimum, will be escorted to sensitive areas.

201. What level of collaboration is expected between the consultant and JMU's internal IT teams during the project?

Answer: The IT Auditor in AMS manages the audits and will assist consultants during the audit. Arranging the entrance conference for each audit and ensuring consultants have what they need to complete the audit (credentials, etc.).

202. In the event that significant risks or vulnerabilities are identified, how quickly can the IT team allocate resources to address them, and what role will the consultants play in the remediation process?

Answer: IT has the resources to address issues identified during an audit. Consultants should notify IT and AMS as soon as possible of significant risks or vulnerabilities as well as providing a recommendation to address the issue(s).

203. How does JMU's IT team currently track and manage vulnerabilities or remediation tasks? Should the consultants integrate with existing ticketing or reporting systems? No

Answer: Will be discussed during planning for each engagement.

204. Is there a preferred ratio of remote to on-site work for projects, or is this determined on a case-by-case basis?

Answer: This is determined during planning.

205. How frequently will status updates or check-in meetings be required during active audit engagements?

Answer: This is determined during planning.

206. For larger projects, is there a preferred team size, or is it acceptable for a single highly qualified professional to perform the audit?

Answer: These audits can be completed by one person.

207. What is the expected format for audit reports and findings? Does JMU have a preferred reporting template?

Answer: The consultant can utilize their own format. We would like to see the scope, audit approach (methodology), findings and recommendations.

208. Is there an established process for presenting audit findings to executive leadership or stakeholders at JMU?

Answer: Audit reports are presented to the Board of Visitors (Audit, Risk and Compliance Committee)

209. Beyond final reports, are interim reports or preliminary findings required during the audit process?

Answer: No, unless determined otherwise during planning.

210. What is the typical turnaround time for report reviews and feedback after submission?

Answer: Could take up to two weeks for AMS to review reports. Typically, one week.

211. How does JMU prioritize remediation actions following audit findings, and is the consultant involved in verifying that corrective measures are implemented?

Answer: Critical issues are directed to IT immediately after discovery. For these issues, the consultant should work with IT to help address the issue.

212. Specify the VLAN detail; how many are included in the scope?

Answer: This will be determined during planning.

213. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

Answer: The university refrains from answering this question.

214. How much (%) of the infrastructure is in the cloud?

Answer: In-scope infrastructure location will be discussed during planning.

215. In the IT department/environment, how many employees work?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

216. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Answer: JMU has multiple server rooms and utilizes some cloud solutions.

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