JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU5759**

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

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

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

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

The contract documents shall consist of:

(1) This signed form;

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

(3) The Contractor's Proposal dated October 23, 2019 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations Summary, dated February 14, 2020.

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

CONTRACTOR:	PURCHASING AGENCY:
By: _____ (Signature)	By: _____ (Signature)
Scott K. Hammer (Printed Name)	Doug Chester (Printed Name)
Title: Client Partner - Public Sector	Title: Buyer Senior

Rev. 10/14/09

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

1. The pricing schedule is as follows:

Teir	Hourly Rate (On-Site)	Hourly Rate (Off-site)
Associate Consultant	$120.00	$100.00
Consultant	$160.00	$140.00
Senior Consultant	$180.00	$160.00
Lead Consultant	$200.00	$180.00
Principal Consultant	$220.00	$200.00

The on-site rate is inclusive of travel.

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

Proposal for

James Madison University

Information Technology (IT)
Security Auditing Services

October 23, 2019

Table of Contents

RFP Cover Sheet

REQUEST FOR PROPOSAL

RFP# FDC-1057

Issue Date: **September 19, 2019**

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

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

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

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

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

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

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

Name and Address of Firm:

Impact Makers, Inc.

3200 Rockbridge Street, Suite 201

Richmond, VA 23230

By: *(Signature in Ink)*

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

Date: October 23, 2019

Title: Principal Consultant – Client Partner

Web Address: Impactmakers.com

Phone: (804) 306-9685

Email: shammer@impactmakers.com

Fax #:

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

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

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

Rev. 2/7/19

I. Introduction and Executive Summary

Department of Information Technology Security Auditing Services Leadership Team,

Below this letter you will find Impact Makers' approach to providing security assessment services for James Madison University (JMU) related to the Virginia Association of State College & University Purchasing Professionals (VASCUPP) RFP# FDC-1057. Impact Makers' team is prepared to partner with the University's Audit and Management Services (AMS) at JMU to identify and address opportunities and challenges to ensure successful security services and solutions.

Why Impact Makers Can Best Support JMU for the Security Assessment Services

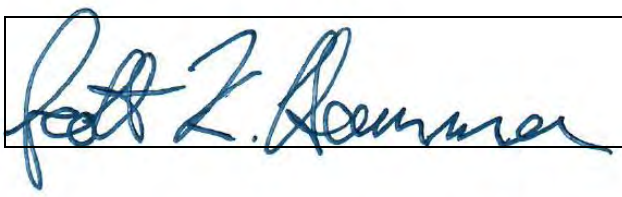
Impact Makers' team understands the importance of a robust security program and consulting services support for JMU and the University's Audit and Management Services. We believe that we can best support the University because:

- 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 a decade of lessons learned, to ensure successful delivery and best outcomes for our clients.
- Our Standards. Impact Makers' IT Security Audit Services conform to the *International Standards for the Professional Practice of Internal Auditing*, issued by the Institute of Internal Auditors (IIA). As required by the IIA, Impact Makers conducted a quality assurance review (QAR) of its IT Security Audit Services through a self-assessment followed by an independent validation. The independent reviewer found that our IT Security Audit Services generally conform to the IIA standards applicable to providing audit services to clients.
- Our Experience. We have provided security assessment for many 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, Virginia State University, the Virginia Department of Elections, and more.
- 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 developed Security Programs, Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity Plans (CPs) for multiple state government agencies and other organizations.
- Our Model. The Impact Makers Model Matters. Simply put, our business model is to support the communities in which we work. *Impact Makers contributes all of its profits over the life of the company and pro bono consulting to charities.* Since 2006, we have contributed nearly $3 million in unrestricted financial support and pro bono management and technology consulting services to nonprofits. 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 brings passion to the transformative work we do for our clients and charity partners.

Thank you for considering Impact Makers (!m) for this project. Enclosed, please find our proposal to provide security assessment services, the focus of which is our experience and expertise in providing the services requested by and our plans to provide these services for the University.

Thank you for considering our proposal. We look forward to the opportunity to discuss our capabilities with you.

Best regards,



Scott Hammer
Principal Consultant – Public Sector Client Partner
C: (804) 306-9685
shammmer@impactmakers.com

II. Background and Summary of Understanding

The purpose of this proposal is to respond to the Request for Proposal (RFP) # FDC-1057 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 Paragraph C of the RFP. Based on our understanding, the University's Audit and Management Services (AMS) is requesting audit support for its IT auditing functions including 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 services related to letters a) through i). 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 organization's needs. In developing project deliverables, we will also leverage our collective experience managing and reviewing state government projects, and deliver the project using consultants with specific expertise in Information Security. With our processes and tools, our experience, and factoring in the unique mission and culture of each organization, we will deliver results that achieve your objectives.

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

> Impact Makers begins each project with a project initiation phase to confirm the project scope and objectives, as well as 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 Agency on project approach, timeline, and key deliverables.

Figure 1 – Impact Makers' IT Security Audits Approach

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.

At the conclusion of each project, Impact Makers completes our collaborative effort with the organization by conducting lessons learned sessions, providing all project deliverables, and closing the project.

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 for state agencies, including developing security policies and procedures. For example, members of our team developed the Commonwealth's SEC501 Information Security Standard, along with associated policies, procedures, and guidelines, and we leverage this experience to develop structured tools that facilitate the assessments. 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.

In addition, as already noted, Impact Makers' IT Security Audit Services conform to the *International Standards for the Professional Practice of Internal Auditing*, issued by the Institute of Internal Auditors (IIA). As required by the IIA, Impact Makers conducted a quality assurance review (QAR) of its IT Security Audit Services through a self-assessment followed by an independent validation. The independent reviewer found that our IT Security Audit Services generally conform to the IIA standards applicable to providing audit services to clients. This conformance provides the University with assurance that the services provided by Impact Makers are fully independent and transparent.

The section below is our plan and methodology to provide services in areas a) through i) 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 assessment services includes similar steps, starting

with a planning phase, continuing with conducting the assessment, and concluding with our reporting findings and recommendations. We detail how we execute these 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 in to many more other areas within anof 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. Plan. This Defining the 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 Agency'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. Assess. Utilizing industry standard tools such as Nmap, Nessus, and OWASP's Zed Attack Proxy (ZAP), the assessment 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. Report Results and Recommendations. 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 contains recommendations for next steps and best practices to help remediate any findings and strengthen the organization's security posture.

B. Wireless Network Assessment

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

1. Plan. 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. Assess. 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. Report Results and Recommendations – 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. Plan. 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. Assess. 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. Report Results and Recommendations. 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. Plan. 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. Assess. 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. Report Results and Recommendations. 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. Plan. 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. Asses. 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 determine 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. Report Results and Recommendations. 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 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. Plan. 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. Assess. Our team assesses the current network scanning process against industry standards such as SEC501, NIST800-53, or other specified by the University, with a focus 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. Report Results and Recommendations. 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. Plan. 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. Assess. Impact Makers utilizes a variety of automated and manual auditing techniques to perform the different application risk assessments required by our clients. 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 (i.e. fuzzing techniques) specific to the known application context.

3. Report Results and Recommendations. Based on the results of the assessment, Impact Makers develops recommendations to improve the 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. Out 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. Plan. 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. Assess. 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 (users, service accounts, etc.) 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. Report Results and Recommendations. Based on the results of the assessment, Impact Makers highlights AD security misconfigurations and recommend 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 Plan-Assess-Report approach, our high-level penetration testing methodology involves four key phases, which may all occur remotely:

1. Plan. In the planning 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 discovery phase, Impact Makers' team 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:
    1. Performing reconnaissance activities, both manual and automated, to discover external-facing assets and IP addresses
    2. Conducting network foot-printing and probing for active devices

3. Performing port scans of systems to identify potential entry points and fingerprint operating system versions and listening services / applications
4. 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
5. Conducting vulnerability scans to identify vulnerabilities present on the network and applications which 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 organization'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:
   1. Kali Linux – penetration testing distribution
   2. Metasploit – open source penetration testing framework
   3. Burp Suite – platform for performing security testing of web applications
   4. Zed Attack Proxy – proxy for performing web application testing
   5. Wireshark – network packet capturing tool
   6. Ettercap – toolset for Man-in-The-Middle (MiTM) attacks

4. Report Results and Recommendations. 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.

IV. Expertise and Qualifications

The below section is a written narrative statement to address the expertise, qualifications, 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

Impact Makers has worked with dozens of state agencies in Virginia, including providing consulting and security assessments for:

- Library of Virginia
- Virginia State University
- University of Virginia Health System
- VCU Health System
- Virginia Information Technologies Agency
- Virginia Department of Transportation
- Virginia Department of Motor Vehicles
- Virginia Department of Health
- Virginia Department of Social Services
- Virginia Department of Elections
- Virginia Alcohol Beverage Control
- Virginia Department of Behavioral Health and Disability Services
- Virginia Department of Education
- Virginia Department of Environmental Quality
- Virginia Indigent Defense Commission
- Virginia Department of Planning and Budget
- Supreme Court of Virginia
- Virginia Hospital and Healthcare Association
- Virginia529 College Savings Plan

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 public sector clients. In particular, we would draw your attention to the client success stories that are documented beginning on page 14. The text of these stories is also included in the Appendix of this proposal.

B. Certifications

Impact Makers' security team members hold the following certifications:

- Certified Information Systems Security Professionals (CISSP) – 7
- Certified Information Systems Manager (CISM) – 7
- Certified Identity Governance Expert (CIGE) – 1
- Certified Information Systems Auditor (CISA) – 3
- Certified in Risk and Information System Controls (CRISC) – 5
- Certified in the Governance of Enterprise IT (CGEIT) – 1
- Certified Public Accountant (CPA) – 2
- Certified Internal Auditor (CIA) – 1
- Certified IT Professional (CITP) – 1
- Information System Security Manager Professional (ISSMP) – 1
- Computer Hacking Forensic Investigator (CHFI) – 1
- Certified Ethical Hacker (CEH) – 1
- GIAC Systems and Network Auditor (GSNA) – 1
- Project Management Professional (PMP) – 5
- Scaled Agile Framework (SAFe) – 4
- Certified Associate in Healthcare Information and Management Systems (CAHIMS) – 6

- Certified Professional in Healthcare Information and Management Systems (CPHIMS) – 1
- HIMSS Analytics Certified Consultant – 3
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) Practitioner – 1
- Six Sigma Green Belt - 2
- ITIL Foundation – 2

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

Project Qualifications begin on the next page.

VIRGINIA STATE UNIVERSITY ▪ IT SECURITY AUDITS

WE HELPED VIRGINIA STATE UNIVERSITY

IDENTIFY CONTROL WEAKNESSES AND MEET COV REQUIREMENTS

OUR CLIENT'S CHALLENGE

Virginia State University, 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. 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 and 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 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.

IMPACT AND RESULTS

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

VIRGINIA 529 ▪ IT SECURITY AUDITS

WE HELPED VIRGINIA 529

TAME THE TUITION MONSTER THROUGH IT SECURITY AUDITS

OUR CLIENT'S CHALLENGE

Virginia529 started in 1994 when the Virginia General Assembly authorized a program to help citizens save for the increasing costs of higher education.

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.

IMPACT AND RESULTS

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

Figure 2 – Impact Makers' IT Security Project Qualifications

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 a Principal Consultant who serves as Client Partner in leading Impact Makers' delivery of services to clients in the public and not-for-profit sectors. He has 35 years of experience in state and Federal government, financial services, higher education, and retailing in many specific areas of expertise, including:

- Organizational transformation and strategic planning
- Human Capital Management
- Business Process Assessment, Design, and Improvement
- Business and Enterprise Performance Management
- Program and Project Management
- Information Technology Risk Management and Security
- 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

Recent Professional Experience

Principal Consultant

Impact Makers, Inc., Richmond, VA (2016 – Present)

- Led a transformational information security project for the Virginia Department of Motor Vehicles. Project included developing 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 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 correctional facilities 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.
- Worked with staff, Board, and other stakeholders to develop transformational strategic plan for Family Lifeline (FLL), a private social services agency, to optimize current organizational capacity and identify areas for capacity improvement. Worked with FLL strategy execution teams to structure initiatives around several accelerator initiatives to enable increases in capacity.
- Developed transformational strategic plan in conjunction with Board, staff, and stakeholders of Wintergreen Performing Arts, an organization that presents musical performances and provides musical instruction at the Wintergreen Resort. Plan enabled the organization to identify and begin execution of initiatives needed to expand the organization's mission.
- Worked with executive director, Board, and staff to develop a strategic plan for Richmond Culture Works, an arts and culture advocacy group. Helped to transform the entire Culture Works Strategy through a series of projects, including defining KPIs and strategic objectives to create a measurable progress scorecard and creating a strategic plan to transition in new board.

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. Developed consensus among agency management regarding essential agency business functions; used this consensus to guide development of Business Impact Analyses, Risk Assessments, Business Continuity Plans, Risk Management Plans, and supporting IT security documentation.
- 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 and directed evaluation and documentation of the core business applications for a public-sector emergency management agency. This evaluation and documentation enabled the agency to correct performance issues with the application and to function effectively during hurricane season.
- 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.
- Managed a diverse team of consultants, vendors, and employees in the build-out of a new data center, network infrastructure, and network cabling plant for a 1,500-person New York City-based law firm, in support of the firm's move to new offices. Completed the project on time, enabling the firm to avoid $1,000,000 in potential penalties, and managed the move of the firm's infrastructure to the new offices with no unscheduled disruption to service.
- Key participant in the negotiation of a comprehensive outsourcing agreement between a consolidated state IT infrastructure agency and its outsourcing partner. Project resulted in consummation of a $2.5 billion, ten-year contract for the outsourcing partner to assume operation of all IT state IT infrastructure.
- Performed analysis of comparative telecommunications costs for a top-ten commercial bank as a key participant in a cross-functional team that developed and implemented a strategic sourcing initiative. Determined competitive costs and negotiated rate improvements with vendors, enabling the bank to realize $15 million in cost savings over three years.

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.
- Managed compliance with Federal information security standards at a cabinet-level Federal agency. Designed and implemented a program for ongoing security audits of all sensitive information systems. Led execution of the program, including regular scanning of all network devices and remediation of all vulnerabilities. Program resulted in the agency's experiencing no reportable information security incidents during an entire fiscal year.

Education and Certifications

M.A., English, State University of New York, Binghamton, NY
B.A., English; minor, Computer Science and Mathematics, Harpur College (SUNY), Binghamton, NY
Project Management Professional, PMI; Six Sigma Green Belt, Oriel, Inc. ISACA, PMI, AITP Certified Information Security Manager, Certified in Risk and Information System Controls, ISACA;

Shannon Yeaker, PMP, CISA, CAHIMS — Lead Consultant

Professional Background

Dynamic IT professional with extensive experience in risk, controls, project and process management in the financial services and healthcare industries. Proven ability in managing large scale organizational efforts and multiple projects across various disciplines. Substantial risk and information security consulting skills. Extensive experience deploying Cisco ISE.

- Portfolio and Project Management
- Strategic Advisor
- Agile Coach / Certified Scrum Master
- Leadership
- Governance, Risk and Compliance
- Data Governance
- Business Process Management
- Relationship Building

Professional Experience

Lead Consultant

Impact Makers, Inc., Richmond Virginia (May 2015 – Present)

- Served as a project manager, subject matter expert and advisor for several projects at two multi-billion-dollar healthcare systems
- Projects focused on service level management, business continuity management, Information Security Architecture and a complex Cisco Identity Service Engine (ISE) implementation
- The projects utilized ITIL, SABSA, BSIMM, OWASP, NIST, HIPAA and PCI standards and frameworks
- Provided thought leadership and direction to the CISO of one healthcare system and the CIO and Security Manager of another healthcare system
- Partnering with the Data Governance Practice Lead to develop the data governance framework and materials

Sr. Manager, Technology

Capital One (August 1994 – May 2015)

- Managed the 2nd level data validation effort of the Hadoop Ecosystem for Enterprise Data Management
- Partnered with the Data Governance and Strategy teams to identify gaps and develop remediation strategies for Hadoop
- Provided recommendations for enhancements to the Information Data Management Policy and Data Quality Standards
- Managed the Technology Operations Chief of Staff Office supporting the Technology Operations leadership to effectively drive organization initiatives, manage horizontal operational activities and to communicate business imperatives across a 1500-person organization
- Drove vital initiatives to empower associates to excel personally and professionally implementing the new IT Job Architecture, managing Performance Management and the College New Hire and Intern Programs
- Heightened organizational visibility and provided thought leadership to the department by facilitating monthly Performance Reviews with Senior Leadership, compiling quarterly Business Reviews for Executive Leadership and managing quarterly Town Halls for the entire department
- Created and enhanced the Technology Operations presence through targeted and timely communication for large scale initiatives such as the Meadowville Data Center Grand Opening

Sr. Process Manager, Capital One Bank

- Program Manager for the bank integration effort in Network Management
- Developed integrated design process for all design deliverables in the branch New Build process that enabled the construction of physical bank branches
- Actively managed, monitored and reported Network Management activities to rebrand ING Cafes to Capital One 360
- Managed, monitored and reported all design deliverables for bank branches to increase process efficiency for the New Build process
- Received nomination for Q3 2012 Bank Leadership Award

Sr. Process Manager, Enterprise Architecture

- Enterprise Architecture process owner for the Basel II Data Quality Validation process
- Defined, managed and monitored the quality assurance process to report the level of data quality across Basel and the Enterprise to ensure corporate compliance to Basel II and other data quality regulations
- Documented processes and procedures for Enterprise Architecture including the Data Quality Risk Dashboard process to streamline the efficiency and effectiveness of reporting for the department
- Accountable for assessing data quality for over 700 data stores across the enterprise to ensure corporate compliance to data quality regulations

Sr. Risk Manager, IT Risk Management

- IT Risk Operations Program Owner for the execution of the IT Controls Program and Subject Matter Expert for the project management processes and Information Data Management and Information Security policies and standards
- Planned, directed and coordinated all aspects of the quarterly IT controls testing across five divisions with onshore and offshore resources to ensure regulatory compliance
- Provided consulting and advisory support to three departments in the areas of risk, controls, audits and waivers
- Provided consulting and advisory support to IT departments in the areas of project management, Information Data Management and Information Security to provide education, drive overall compliance and to help reduce risks to an acceptable level for the organization
- Awarded Associate of the Quarter for a 300-person department in Q4 2009

IT Project Manager & Agile Coach, Compliance IT

- Agile Coach, Delivery Lead and Risk and Controls Lead for the Anti-Money Laundering team
- Coached a team of technology and business professionals for the delivery of projects, enhancements and platform management activities for several platforms with distributed resources to meet the department's delivery targets and reduce organizational risk
- Promoted risk and controls by ensuring adequate education and controls were in place at the team, project and platform level to enhance compliance to regulatory requirements
- Promoted process and project management methodologies to enhance education and to drive process efficiency across the team
- Led the change management effort to implement a new project management tool for a large division to ensure the divisions' project resources could effectively execute on projects in the new tool
- Received prestigious Circle of Excellence award for Regulatory IT Project
- Received prestigious Circle of Excellence award for developing a new IT project management process
- Received Process Excellence award for work with IT Solutions Delivery process development

IT Project Manager, Risk IT

- IT Project and Portfolio Manager supporting Fraud and Collections
- Executed on the Collections IT Portfolio by delivering projects on time, within budget and according to business objectives to ensure the delivery of prioritized projects
- Planned, managed and directed activities and resources to ensure the project goals and objectives were accomplished on time, within budget and met business objectives while ensuring customer satisfaction with the Fraud business unit
- Trained project management staff on the project management methodology, tools and communication protocols to increase effectiveness of the delivery organization

Consultant and Compliance Analyst, Information Security and Business Continuity Management

- Consultant and Compliance Analyst for four business ventures
- Identified risks and remediation strategies for the new credit card business in France by collaborating with information security risk experts across Europe to ensure compliance to regulatory requirements
- Defined security requirements for the prepaid cellular business to ensure the new business complied with regulatory requirements
- Identified risks and remediation strategies for the Canadian outsourcing effort by analyzing the business processes and assessing the physical security of the vendors to ensure the new business relationship complied with regulatory requirements
- Identified risks and remediation strategies for potential IT and Call Center partners in India to ensure our vendors complied with regulatory requirements

---

Education and Certifications

Bachelor of Science, Psychology– James Madison University
Master's Certificate, Project Management – George Washington University

Project Management Professional (PMP)
Certified Information Systems Audit (CISA)
Certified Associate in Healthcare Information and Management Systems (CAHIMS)
Business Process Management Certification
Capital One Certified Agile Coach
Certified Scrum Master
Lean Certification

Professional Development, Community Involvement, Skills, Awards, Publications, etc.

- Blog Post, August 2018 "GDPR is Here! What is it and How Does it Affect Your Compliance Management Program?
- STEAM Speaker, 2017 Conference Richmond, Virginia
- RVASec Speaker, 2017 Conference, Richmond, Virginia
- Two Time 'Circle of Excellence' Award Recipient, Capital One
- Process Excellence Award

Ron White, CISM, CAHIMS, CCNP — Lead Consultant

Professional Background

Ron is a Senior Level Information Security and Governance, Risk, and Compliance leader, successful at building high performance teams to build and address Information Security Programs for multiple diverse organizations within both the public and private sector. He is a strategic visionary with a clear sense of purpose and urgency when faced with the decisions regarding the protection of corporate assets. Ron has proven success engineering, delivering, and managing complex technology and security solutions and business operations. He is a highly energetic individual with superior interpersonal skills that can translate complex technical and security terms to common business language. He has extensive experience working with clients, managing projects to completion, delivering work products, and maximizing team productivity. Ron has high-caliber presentation, negotiation and communication skills.

His professional strengths include:

Executive Oversight
Vision, Strategy & Execution
Organization Development
P&L / Operations Management
Budgeting & Cost Control
Team Building, Mentoring & Leadership
Contract Negotiation & Vendor Relations
Compliance & Regulatory Management
Corporate Communications & PR
Internal & External Customer Relations
Risk Management
Security Governance

Strategy & Execution
Strategic & Countermeasure Planning
Vulnerability Project & Program Management
Security Operations Center
Business Continuity & Disaster Recovery Planning
Project Planning & Management
Internal Relationship Building
Change Management & SDLC
Security Policy & Standards Development
Systems Audit & Control
Incident Management & Response
Data Center Operations

Areas of Expertise

Security/Risk Management Leadership
- Define, develop and communicate Security and IT risk management standards and concepts
- Consult with senior executives in healthcare, financial, and governmental organizations to comply with federal and state regulations and to design and deliver a roadmap, strategy, and projects to meet those regulations.
- Develop metrics to analyze and improve security programs
- Establish and oversee Business Continuity (BCP) and Disaster Recovery Planning
- Apply Program and Project Management skills to lead and manage complex, high-impact projects
- Develop and implement Enterprise Security Architecture for addressing risks to the confidentiality, integrity, and availability of data

Security/Risk Management Practice
- Define organizational risk appetite, design and implement risk policies and governance
- Design, implement and manage Security & Risk Management tools & systems, statistical models & expert IT risk teams
- Identify, analyze, measure, and communicate complex threats and risks to multiple stakeholders
- Design and develop Security and BCP Assessment tools for ensuring compliance with mandated regulations

Professional Experience

Lead Consultant
Impact Makers, Richmond, Virginia (July 2017 – present)
Consulted, solved problems, and added value with both public and private clients as a Lead Governance, Risk, and Compliance Consultant with emphasis in the following areas:
- Strategized with potential clients and architected and delivered solutions
- Designed and updated security programs for large financial and healthcare organizations
- Provided security and leadership training to all levels of an organization

- Consulted with senior executives on federal, state, and European regulation compliance, including SOx, GDPR, DFS 500, and FFIEC
- Developed information security and policy frameworks aligned with client's corporate strategy and risk posture
- Defined processes for the assessment, mitigation, and reporting of risks
- Identified and presented threats, risks, and recommended action plans to large, complex organizations
- Led multiple teams to accomplish client goals and objectives using accepted project methodologies
- Provided leadership and mentoring to team members.

Senior Consultant

Impact Makers, Richmond, Virginia (September 2013 – June 2017)

Consulted, solved problems, and added value with both public and private clients as a Senior Governance, Risk, and Compliance Consultant with emphasis in the following areas:

- Created engagement strategy for clients and led teams through the fulfillment of the project requirements.
- Worked with clients to validate that all services and deliverables met expectations.
- Developed internal processes and templates to improve quality and reduce costs.
- Understood clients' needs and discussed additional service offerings to meet those needs.
- Reviewed contracts to verify that the forecasted delivery hours would meet contract objectives.
- Provided expertise in the following areas:
  - HIPAA, NIST 800-53, SEC501, and ISO 27001 Compliance
  - Business Impact Analysis
  - Risk Assessments
  - Security Audits
  - Continuity and Disaster Recovery Planning
  - Policy and Procedures
  - IT Governance and Data Management

CISO/Director of Security and Business Continuity

Estes Express Lines (August 2012 – August 2013)

Performed duties as the executive-level leader of Information Security, Network Security, Business Continuity and Disaster Recovery for this large International Trucking Company. Given full autonomy of the design, development, implementation, and oversight of the security program.

- Built and organized a security program at Estes where none existed previously. Provided thought leadership and communicated security trends to executive leadership.
- Created vision and wrote a security framework. Provided new policies and procedures to improve information security awareness and compliance.
- Coordinated the efforts of HR and other business units to standardize employee titles and their roles and responsibilities.
- Created and staffed a new Release Management program at Estes. Reviewed and restructured source code repositories and the processes to get development code into production.
- Analyzed systems and processes for risks and threats. Initiated and completed multiple projects to improve the security posture of multiple systems and processes.
- Provided guidance and an architecture roadmap for ongoing and future projects to improve and maintain security best practices.
- Created and managed a multi-million-dollar security budget.
- Worked with multiple business units to discuss and improve business continuity strategies.

Director of Infrastructure and Operations

Estes Express Lines (October 2010 – August 2012)

Executed responsibilities as a senior IT leader of Data Center operations, Asset Management, Field IT support and Telecommunications, and Help Desk Management.

- Orchestrated the modernization of Estes' datacenter with new hardware, software and processes. Created and developed Estes' technology strategy and vision.
- Analyzed and made final purchasing decisions on hardware and software purchases. Developed, with vendors, business value presentations for C-level executives.
- Directed the update of Active Directory and Citrix environments and the migration of thousands of employees to new hardware and systems
- Negotiated contracts and pricing with hardware, software, and services vendors. Saved Estes millions by renegotiating existing hardware, licensing, and telecom contracts.
- Managed and monitored internal licensing compliance for software vendors. Made executive decisions on how to improve Estes' ROI using different licensing agreements.
- Coordinated the standardization and automation of many time-consuming and manual processes for the computer operations team,

improving their efficiency 300%.
- Restructured and improved the skillset of the help desk personnel. Enforced the documentation of common issues to improve resolution time. Purchased and oversaw the installation of a new ticketing system, which improved ticket routing and resolution time.
- Directed the work of 7 managers with more than 65 subordinates.
- Initiated and organized a project to migrate thousands of employees from Lotus Notes to Microsoft Exchange.
- Created and managed a 15- to 20-million-dollar infrastructure and operations budget.

Director of IT

InteliTap, LLC (January 2007 – February 2010)

Directed and performed work as the senior IT leader of a startup company. Responsible for Project Management, Datacenter Operations, Field Support, Application Design and Development, and Customer Experience.

- Provided technical expertise and oversight in project management, server and database administration, risk management, process improvement, network and firewall configuration, business strategy, vendor management, and disaster recovery. Identified critical path decisions and provided continual cost/benefit analyses and recommendations for new software and hardware designs.
- Clarified and customized processes and procedures for help desk and operational support staff to facilitate reduced cost and enhanced customer relationships. Wrote training and support manuals for employees and customers. Implemented a web-based incident tracking system and oversaw performance metrics.
- Designed, built, and managed foreign and domestic data centers. Established best practices for data backup and resource optimization. Led multiple teams to resolve production issues.
- Coordinated and managed foreign and domestic Java development teams, including contractors, using Agile methodologies as the Scrum Master/Project Manager. Developed and implemented comprehensive project plans, managing resources, costs, and schedules. Moved development team in-house reducing development time and production issues by 70%.

Data Center Manager

Virginia Department of Social Services (January 2005 – January 2007)

Performed duties as a Technical Services Manager responsible for Datacenter Operations, Telecommunications, and Vendor Management of this large State Government Agency.

- Managed a 12,000-user network with over 200 offices. Led a 12-man team responsible for 200+ Windows and Linux servers, 700+ Cisco firewalls, routers, switches, and VOIP/Unity equipment. Conducted feasibility studies for future growth and tactical planning. Consulted with executives about purchasing hardware and hiring personnel.
- Defined all aspects of multiple domains including controllers, active directory, permissions, backups, and hardware replacements. Monitored server and network infrastructure, analyzed traffic. Developed processes and procedures to reduce unnecessary bandwidth usage.
- Managed concurrent projects developed mechanisms to achieve objectives. Monitored project progress using milestones and master plans.

Network Technician

Virginia Department of Social Services (June 2000 - December 2004)

Team Member responsible for Network Operations and PC Support

---

Education and Certifications

Master of Business Administration in Information Systems; Virginia Tech, Blacksburg, VA
Bachelor of Science in Management; Brigham Young University, Provo, Utah

- ITILv3
- CCNP
- MCSE
- CAHIMS
- CISM

Ryan Meglathery, MBA — Senior Consultant

Professional Background

High achieving leader with a dynamic history of leading daily execution of Information Technology (IT) functions—security, business applications, project management, and operations maintenance and support. Integral contributor with a critical role in achieving the organization's objectives for customer growth. Strong track record of formulating and implementing technology strategies and direction for complex projects. Skilled in collaborating with multiple stakeholders to define the current and future state of business processes, identifying issues and risks, suggesting mitigation strategies, and driving towards improved technology solutions. History of progressive responsibility has resulted in generated revenue, improved employee culture, and streamlined operations while increasing the bottom-line.

- Payment Card Industry (PCI) Expertise
- Security Strategy
- CISO
- Information Technology Risk Strategy
- Cross-functional Team Leadership
- Articulating Complex Concepts in Simple Language
- New Technology Integration
- Startup Board of Directors Officer
- Non-Profit Technology Advisor
- Leadership
- Program Management
- Penetration Testing/Ethical Hacking
- Project Management
- Mentoring Senior Staff
- Act as a Conduit between Technical and Executive Levels
- Relationship Building
- Budget and Resource Planning
- Non-Profit Board Membership

Professional Experience

Senior Consultant
Impact Makers, Inc., Richmond Virginia (April 2019 – Present)
- Provide information security, technology, and strategy consulting services to Impact Makers' clients
- Provides strategic consultation as well as specialized deep technical consulting
- Co-created penetration testing capability at Impact Makers
- Designed and developed penetration testing methodologies
- Specified the requirements for the development of systems used for penetration testing and vulnerability assessments.
- Leverage over a decade of experience in vulnerability assessments and penetration testing to deliver accurate, timely, and thorough assessments

Excellens Consulting, LLC
Owner/Principal Consultant (September 2017 – April 2019)
- Identified early business opportunities, resulting in earnings of $55K+ within first 6 months of operations
- Standardized security initiatives and CISO responsibilities for numerous executive clients
- Assisted a local startup with PCI network architecture design and overall business strategies
- Designed the front and backend of a SaaS solution comprised of mobile and web-based applications using an Agile framework
- Helped a non-profit with pro bono product design and interactive mobile application development

Xenith Bankshares
Vice President of Security/Department Head/CISO (January 2017 – January 2018)
- Developed all information security strategies and policies and oversaw the corporate IT risk advisory and program alignment
- Coordinated the department budget and assisted with management of the overall IT budget
- Provided updates on key metric to executive stakeholders
- Transformed an inefficient program to support a $3B managed assets merger.
- Key player on numerous executive boards, including the IT Steering Committee.
- Revamped the information security program, standardizing new processes and policies, assigning quantitative value to IT risks, incorporating a new information security program roadmap and associated tools.
- Successfully streamlined operations and decreased operating and employee costs.
- Mentored junior staff, providing custom training to fill crucial skill gaps.

AppSec Consulting
Team Lead (January 2015 – January 2018)
- Led consultant team tasked with delivering custom information security solutions, such as PCI, HIPAA/HITECH, NIST, ISO, FFIEC, and HITRIST CSF
- Executed penetrating testing and developed overall client security plans
- Created security program strategies and services and for clients in multiple industries
- Named project lead on engagement worth in excess of $2 million in revenue
- Created a database-powered PCI DSS 2.0 assessment and reporting tool and a HIPAA assessment tool, driving efficiency by 25%

CBIZ Security & Advisory Services, LLC
Team Lead (January 2015 – January 2018)
- Delivered strategic, advisory, and information security assessments, overseeing and prioritizing tasks for 3 consultants
- Created security program strategies and services and for clients in multiple industries
- Named project lead on engagement worth in excess of $2 million in revenue
- Created a database-powered PCI DSS 2.0 assessment and reporting tool and a HIPAA assessment tool, driving efficiency by 25%
- Designed a penetration testing service offering, increasing revenue by 15% annually

Senior Security Consultant
Fortrex Technologies, Inc. (2010 – 2013)

Security Consultant
Verizon Business (2005 – 2010)

Assistant Vice President/Information Security Lead
JP Morgan Chase (2003 – 2005)

Security Consultant
Global Integrity (1998 – 2002)

Education & Certifications

MBA, Entrepreneurship & Leadership, University of Virginia Darden Graduate School of Business, Charlottesville, VA
Bachelor of Interdisciplinary Studies, Liberal Arts, University of Virginia, Charlottesville, VA (summa cum laude)

Professional Development

- Certified Information Systems Security Professional (CISSP), (ISC)²
- Certified Ethical Hacker
- Former Payment Card Industry Data Security Standard (PCI-DSS) Qualified Security Assessor
- Former PCI Payment Application Data Security Standard Qualified Security Assessor (PA-QSA)
- Former HITRUST Certified Common Security Framework Practitioner (CCSFP)

Community Involvement

- Treasurer and Board Director, Kangy, Inc.
- Former Board Member and Director of Technology, WagiLabs
- Former Chief Operation Officer, MBA Entrepreneurship Club, University of Virginia
- Former Director of IT, Richmond Chinese School Board of Director
- Former Board Member, Alpha Sigma Lambda Honors Society

Mark Cannon, CISSP, CISA, CPA — Consultant

Professional Background

Mark is an Information Security, Audit, Risk, and Compliance professional with experience in the Pharmaceutical, Healthcare, Finance, Telecommunications and Government sectors. He has worked extensively across business disciplines with teams from audit, accounting, finance, treasury, legal, marketing, security, sales, and information technology. Mark ensures compliance with GAAP, Commonwealth of Virginia Information Security Standards, HITECH Act, HIPAA Security Rule, SOX, GDPR, FFIEC and FDIC utilizing NIST Cyber Security, ITIL, COSO, and COBIT frameworks.

- Compliance
- IT Governance
- Contract Administration
- IT Controls
- Financial Controls
- Operational Controls
- SOX Controls
- Internal Audit
- Risk Management
- Information Security

Professional Experience

Consultant
Impact Makers, Inc., Richmond, Virginia (April 2019 – Present)
- Working with management to ensure IT controls are in place to meet business needs.

Senior Compliance Analyst
Indivior, Richmond, Virginia (July 2018 – March 2019)
Indivior is a $1B specialty pharmaceuticals business focused on addiction treatment.
- Worked with Information Technology and Finance Managers to ensure appropriate controls associated with financial reporting and SOX ITGC are in place.
- Managed weekly Change Control Board Meetings reviewing evidence and scheduling moves to production.
- Supported SAP, Workday, Success Factors, Infrastructure and Security teams in IT governance activities and contract administration.
- Lead mitigation efforts and prepare monthly reports to key stakeholders and senior management on status of compliance efforts.
- Created and updated Governance Policies and Standard Operating Procedures.

Senior IT Analyst
Bon Secours, Richmond, Virginia (February 2015 – June 2018)
Bon Secours is a $3B hospital system managing 13 hospitals and providing EHR cloud services.
- Served as Analyst and Project Manager for Enterprise Data Center supporting the Information Security Program implementing controls over 1500 servers.
- Worked with 20+ Systems Engineers in implementation of systems, maintenance and monitoring of security systems and processes.
- Provided guidance on the information security program and policies.
- Mentored WinTel, Citrix and Unix system engineers on information best practices related to security infrastructure, including audit logging, patch management, server hardening, trust framework, malware protection, change management, access controls, assessing threats, risks, and vulnerabilities.
- Developed guidelines for privileged account management and server configurations.
- Prepared System Security Plans.
- Assisted with computer incident response, operational, and risk and vulnerability assessments.
- Worked with external auditors evaluating IT general controls for financial and SOC2 audits.

IT Risk Manager
Capital One, Richmond, Virginia (June 2013 – December 2014)
Capital One is the 10th Largest bank in the US with $363B in assets.
- Worked with Information Security providing risk management expertise advising on technology and management policies, standards and processes.
- Participated in audit reviews and risk management of the Commercial Banks 100+ applications.

- Managed mitigation activities ensuring that the appropriate information security processes and assessments are followed.
- Partnered with the internal stakeholders to resolve audit issues.
- Provided regular reporting to communicate the status of risk and compliance actions to appropriate individuals within the organization.
- Prepared application risk assessments that included a comprehensive view into application-level risks.
- Coordinated Operational and SOX audit activities with the application support teams.

IT Audit Manager

SunTrust Bank, Richmond, Virginia (May 2011 – May 2013)

SunTrust Bank is the 17th largest bank in the US with $211B in assets.

- Lead in general and business control audits of consumer banking and mortgage technologies and back office processing.
- Developed integrated audits plans and procedures with financial and operational auditors using risk-based assessment of systems;
- Reviewed enterprise project management, risk management, data governance, vendor management, systems processing, and network and database security and recovery controls.
- Monitored and reported on management mitigation efforts to close significant audit issues to ensure compliance with federal regular findings.

Senior Accountant

Cavalier Telephone, Richmond, Virginia (June 2010 – May 2011)

Cavalier Telephone, a subsidiary of Windstream, provides telephone and internet service in the Eastern US.

- Assisted the Controller in responding to external auditors6 and performing special assignments;
- Developed documentation of accounting processes;
- Performed queries on data bases to extract financial records;
- Created trial balances, schedules and financial statements; reconciling accounting systems;
- Developed procedures for updating accounting databases.

Internal IT Auditor, Internal Audit Manager & Internal Audit Director

Virginia Lottery, Richmond, Virginia (September 1989 – June 2010)

Virginia Lottery provides entertainment and annual revenues of $600M for Virginia Schools K to 12.

- Internal Audit Director leading the internal audit program.
- Managed and performed audits that included: compliance, operational, IT and financial reviews;
- Worked with management as an advisor regarding information systems management and financial accounting on all matters involving internal controls and enterprise risk management, policy and procedure development, internal service delivery, financial accounting standards, information systems security and best management practices.
- Participated as a member of the Information Security Committee in development of policies and procedures to ensure compliance with Federal and Commonwealth of Virginia (COV) Information Security Standards.
- Prepared the Internal Audit Department's budget; development of annual and four-year audit plans.
- Managed Audit Committee meetings.
- Directed and assisted in the development of the Agency Risk Management Internal Control program for compliance with governmental accounting and auditing standards.
- Directed and assisted in special projects involving cross-department teams to address strategic initiatives to maximize operating efficiencies; participating in the strategic planning process and analysis critical strategic issues.
- Prepared and presented briefings to the Board of Directors and executive management team.
- Conducted peer reviews of internal auditors.
- Served as a hearing officer to ensure retailer compliance with State laws and regulations.

Education & Certifications

Bachelor of Science, Accounting, Christopher Newport University, Newport News, VA
Certificate in Healthcare Informatics, Boston University, Boston, MA

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Public Accountant (CPA)

Zachary Ugol — Consultant

Professional Background

Zach is a consultant with three years of experience helping companies to assess IT risks and develop controls frameworks. Zach has performed information security and business process audits in accordance with SOX, SOC 1 / SOC 2 / SOC 3 requirements, and Commonwealth of Virginia SEC501 standards.

Functional Expertise
- IT Risk Assessments & Gap Analysis
- IT Security Audits
- Deficiency Response Plans

Key Industry Experience
- Financial Services
- Power / Utilities
- Not-For-Profit
- Public Sector

Professional Experience

Consultant
Impact Makers, Inc., Richmond Virginia (March 2019 – Present)
- Consulting with management on risk mitigation strategies and identifying control solutions
- Developing risk-based system project audit strategies and programs in collaboration with subject matter experts
- Working on audit work papers for compliance with client security policy and standards including Sarbanes Oxley, SOC 1, SOC 2, SOC 3, SEC501, and SEC525.
- Developing data analysis and continuous auditing strategies as requested
- Effectively presenting conclusions in both written and verbal form to Practice Leadership and our clients' senior management with the risk perspective of our clients' audit committees.
- Creating strategies for remediating audit findings commensurate with business risks and needs
- Facilitating client workshops to understand audit findings and begin to develop detailed remediation plans
- Coordinating across multiple teams to meet client goals and objectives using accepted project methodologies

Senior Associate
PricewaterhouseCoopers, Richmond, Virginia (June 2018 – March 2019)
- Assessed the design of IT and business process internal controls in accordance with regulatory guidance and auditing standards (Sarbanes Oxley, SOC 1, SOC 2, and SOC 3)
- Recommended process enhancements and risk management strategies based on industry and technical expertise
- Designed detailed testing plans of controls based on technical and system requirements
- Developed and managed project plans to effectively utilize staffing resources
- Strengthened client relationships by being attentive to customer challenges and providing relevant thought leadership and insights
- Provided real time coaching and on the job training to staff
- Assisted clients in risk analysis during system implementations to minimize risk and leverage existing control structures

Experienced Associate
PricewaterhouseCoopers, Baltimore, Maryland (January 2016 – June 2018)
- Developed and documented an understanding of the clients IT general controls
- Executed detailed testing of IT general controls in accordance with regulatory guidance and auditing standards
- Developed technical and industry expertise through attending trainings and networking events
- Assisted clients in fostering collaboration between IT and business departments to encourage IT security awareness

Education and Certifications
Bachelor of Science, Accounting, Ithaca College, Ithaca, New York
Certified Public Accountant (exams passed)
AWS Certified Cloud Practitioner

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 the needs of the client.

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

   Years 13 Months 6

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
Virginia Department of Transportation – Numerous Information Security Projects including Operational Technology Security Assessment	10 years	1401 E Broad St, Richmond, VA 23219	Murali Rao Innovation Office 804-786-9702 murali.rao@vdot.virginia.gov
Virginia State University – Network Infrastructure and Kronos IT Security Audits	6 years	1 Hayden St, Petersburg, VA 23806	Hubert H. Harris Vice President for Administration (804) 524-5070 hharris@vsu.edu
Virginia Department of Motor Vehicles – Numerous Information Security and other projects and Information Security Transformation Program	9 years	2300 W Broad St, Richmond, VA 23269	Beau Hurley Chief Information Security Officer (804) 367-0067 beau.hurley@dmv.virginia.gov
Virginia Department of Social Services – Information Security Audits and numerous other projects	10 years	801 E. Main Street Richmond, VA 23219	Barry Davis Chief Information Security Officer (804) 726-7153 barry.davis@dss.virginia.gov
Supreme Court of Virginia – Risk Assessments, Fractional ISO, Information Security Program Development	6 years	100 N 9th Street, Richmond, VA 23219	Mike Riggs Chief Information Officer (804) 786-6455 mriggs@vacourts.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: ___10/23/19_____
Is your firm a Small Business Enterprise certified by the Department of Small Business and Supplier Diversity (SBSD)?
Yes__X___ No_____
If yes, certification number: ___660781_____ Certification date:_____Expires 12-22-2019_____

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: _____
Is

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: _____ Date Form Completed:_____

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

Offeror / Proposer:

_____ _____ _____

Firm Address

Contact Person/No.

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

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

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.

Impact Makers has not performed work for any of the VASCUPP Member Institutions within the last twelve months. In the past, however, we have delivered successful projects for Radford University, the University of Virginia Health System, and the Virginia Commonwealth University Health System. We have also delivered successful projects for the Library of Virginia and Virginia State University, which, while not VASCUPP members, are a Commonwealth of Virginia institutions of higher education.

VIII. Proposed Cost / Rate Card

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

For each engagement, Impact Makers will determine the level and amount of staffing needed to meet the organizations requirements. Additionally, Impact Makers will coordinate with the client 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. 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.

Tier	Hourly Rate (On-Site)	Hourly Rate (Off-Site)
Associate Consultant	$ 140	$ 120
Consultant	$ 180	$ 160
Senior Consultant	$ 200	$ 180
Lead Consultant	$ 220	$ 200
Principal Consultant	$ 240	$ 220

Figure 3 – Impact Makers' Hourly Rates

IX. About Impact Makers

Why Impact Makers Can Best Support JMU

Impact Makers understands the importance to JMU of these audit projects. We believe that we can best support JMU's audit needs because of our:

- Exceptional consultants who have IT Security Audit and Assessment experience (see Resumes above).
- Extensive experience in conducting assessment and audit services for other Commonwealth of Virginia (COV) agencies.
- Experience developing the Commonwealth of Virginia's IT Security Standard and IT Security Auditing Services that have been assessed as conforming to IIA Red Book standards.
- 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 Qualifications & Reference below).
- A compelling business model – Impact Makers is committed to contributing all profits and pro bono consulting to charities in the Richmond area (see Company Overview below).

Company Overview

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 companies a hundred times our size due to this revolutionary model. As a founding B Corp, we have been named "Best for World" for the past five years, as well as ranking on the Inc 5000 Fastest Growing Companies list for the past six years. We are a certified SWaM small business through the Virginia Department of Small Business and Supplier Diversity and a certified company through the Virginia Values Veterans (V3) Program (see Certifications below).

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.

Founded in Richmond, Virginia in 2006, Impact Makers has contributed over $3 million in unrestricted financial support and pro bono support to our community partners:

- Family Lifeline helps families succeed & assists Central Virginia's most vulnerable children, parents & seniors by providing support, wellness & education.
- Peter Paul Development Center supports the residents of Richmond's East End with education, senior and after-school programs, a food bank and other community resources.
- 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.
- Virginia Association of Free and Charitable Clinics improves healthcare access by supporting, strengthening, and promoting a robust, high-quality free and charitable clinic system and supporting clinic operations
- Homestretch empowers homeless parents with children to attain permanent housing and self-sufficiency by giving them the skills, knowledge and hope they need to become productive participants in the community
- PodiumRVA helps all Richmond youth find a passion for writing and have the opportunity to share their voices and succeed in a modern culture and economy.
- Computers4Kids combines mentoring and technology to prepare youth for brighter futures by equipping diverse youth with STEAM (science, technology, engineering, arts, and math) skills and a future full of choice.

The impact of our business model is demonstrated by the impact our support has had on our charity partners:

"Every day, I am moved by the generosity of Impact Makers. The work that we do at Family Lifeline can be difficult as we work with families who face significant obstacles. Because of the support we receive from the many Impact Makers staff members; we are reminded that we are not alone and that we are becoming a more vibrant, sustainable organization."

Amy Strite, MSW, LCSW – Executive Director, Family Lifeline

"Since 2008, Impact Makers has made a tremendous financial and volunteer investment in RxP, having invested more than $200,000 and 700 volunteer hours. This investment equated to services provided for more than 6,500 uninsured patients throughout Virginia and more than 65,000 prescriptions with a retail value of $15.8 million."

Amy Yarcich, Executive Director, Rx Partnership

"Our partnership with Impact Makers enabled Peter Paul Development Center (PPDC) to provide academic instruction and enrichment for 146 students in grades 2-12 and 90% of students showed improvement in at least one subject during the 2014-2015 academic year. One hundred percent of students also participated in at least one enrichment activity per week and 86% of parents volunteer at least once during the school year.

Peter Paul is a more robust and data-driven organization because of Impact Makers– for this, and for so much more, we thank them! Words cannot express our gratitude for being an Impact Makers' partner. Every day we live our purpose to Educate the Child, Engage the Family, and Empower the Community. With their support, our ability, efficiency, and effectiveness in doing so is greatly heightened."

Damon Jiggetts, Executive Director, Peter Paul Development Center

History

Based in Richmond, Virginia, Impact Makers was founded in October 2006. In 2007, we became a founding certified B Corporation - a business that formally adopts a social mission in addition to pursuing profit. We joined a global group of more than 2,500 organizations committed to benefit the environment and community and use business as a force for good.

Other notable events include:

- For seven years, Impact Makers was on the *Inc.* 5000.
- The Initiative for a Competitive Inner City (ICIC) and *Fortune* magazine recognized Impact Makers for the Inner City 100 awards from 2015-2017.
- Impact Makers was named a Top Workplace by the *Richmond Times-Dispatch* for four years.
- *Consulting* magazine named Impact Makers to their 2017 Seven Small Jewels and 2016 Seven Small Jewels: Seven to Watch lists.
- The Virginia Chamber of Commerce named Impact Makers to their 2017 Fantastic 50 list.
- For the past six years Impact Makers was recognized as 'Best for the World and 'Best for Community' for creating the most overall social, environmental and community impact.

Figure 4 – Impact Makers' Recent Awards

In 2015, Impact Makers gifted the company's equity ownership to two nonprofit foundations. The company is owned 70% by The Community Foundation Serving Richmond and Central Virginia and 30% by Virginia Community Capital (VCC). These organizations created funds that will support charities and invest in B Corps and other companies with social missions.

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 charity partners. The figure below depicts how Impact Makers' business model benefits our clients, non-profit partners, and the community.

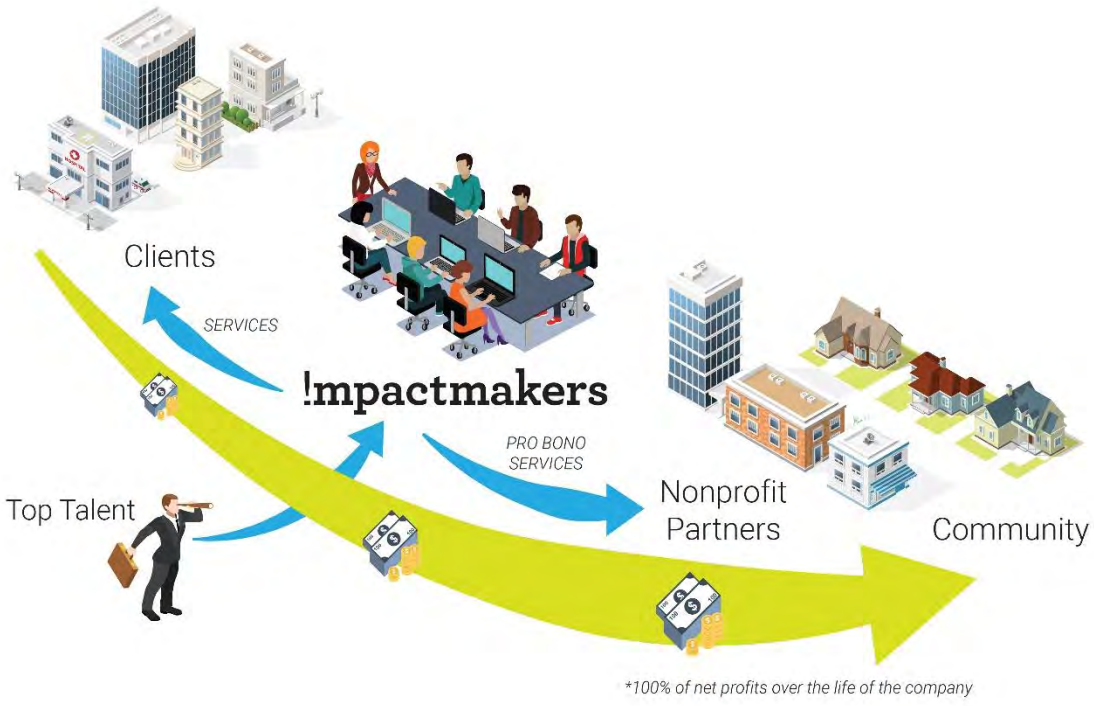


Figure 5 – Impact Makers' Business Model

Our Services

At Impact Makers, we provide a different technology and management consulting experience. We focus on the industries with the greatest amount of change and help private companies and public-sector organizations manage transformations across IT, security, digital, and people.

Figure 6 –Impact Makers' Services

X. Appendix

Qualifications

Virginia Department of Social Services MARS-E Vulnerability Assessment

Impact Makers helps the Virginia Department of Social Services maintain access to their federal exchange.

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 and serving over 1.6 million Virginians each year.

The Challenge

Access to the Centers for Medicare & Medicaid Services (CMS) is a critical component of VDSS's ability to meet its mission and an independent security assessment federally mandated to be conducted every 3 years. This year federal standards changed the game providing a new format and expanded privacy requirements. VDSS needed help understanding the new standards driving completion of the assessment for continued CMS access.

VDSS turned to Impact Makers, the Commonwealth of Virginia security provider of choice, for help in completing the assessment and driving a prioritized plan for continued improvement in their security posture.

Impact Makers' Solution

Impact Makers not only met the new federal standards and assessed the required IT security controls, we developed tools to track the work and provide an evidentiary chain that documented each step of the assessment and testing. These tools provide traceability for CMS reporting, which facilitated a smooth CMS submission. The assessment followed the CMS Framework and Procedures to the letter and the tools captured salient details for the Minimum Acceptable Risk Standards for Exchanges (MARS-E) audit.

As part of the engagement, Impact Makers assessed:

- MARS-E compliance of VaCMS
- Security posture of the underlying infrastructure
- Security posture of the system and data
- Security and proper configuration associated with the database or file structure storing the data as well as the supporting operating system configurations

Our client's Successes

!m successfully helped the customer realize:

- Continued access to the CMS
- A prioritized list for driving security program improvements
- Configuration assessment based on the Independent Assessment Framework and CIS hardening standards
- Security and Privacy Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

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

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, that is committed to the preparation of a diverse population of men and women 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

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. 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 and 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 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.

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 more to offer customers additional choice.

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. A proprietary address validation system that is used to ensure that Virginia529 mailing addresses are accurate.
2. A newly rolled out application that supports Virginia529's Achieving a Better Life Experience (ABLE) Savings program.
3. A system that collects account data for SOAR scholars and applicants.

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, VSU met COV information security requirements. In addition, Virginia529 improved control effectiveness in several areas.

JAMES MADISON UNIVERSITY

Request for Proposal

RFP# FDC-1057

Information Technology (IT)
Security Auditing Services

September 19, 2019

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

REQUEST FOR PROPOSAL
RFP# FDC-1057

Issue Date: **September 19, 2019**

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

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

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

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

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

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

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

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature in Ink)

Name: _____
(Please Print)

Date: _____ Title: _____

Web Address: _____ Phone: _____

Email: _____ Fax #: _____

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

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

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

REQUEST FOR PROPOSAL

RFP # FDC-1057

TABLE OF CONTENTS

I. PURPOSE

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

II. BACKGROUND

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

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

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

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

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

IV. STATEMENT OF NEEDS

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

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

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

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

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

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

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

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

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

D. Billing Rate:

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

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

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

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

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

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

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

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

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

3. Proposal Preparation

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

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

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

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

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

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

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

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

B. SPECIFIC PROPOSAL INSTRUCTIONS

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

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

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

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

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

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

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

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

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

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

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

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

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

VII. GENERAL TERMS AND CONDITIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

J. PAYMENT:

1. To Prime Contractor:

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

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

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

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

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

2. To Subcontractors:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

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

2. Employer's Liability: $100,000

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

X. E-VERIFY REQUIREMENT OF ANY CONTRACTOR: Any employer with more than an average of 50 employees for the previous 12 months entering into a contract in excess of $50,000 with James Madison University to perform work or provide services pursuant to such contract shall register and participate in the E-Verify program to verify information and work authorization of its newly hired employees performing work pursuant to any awarded contract.

VIII. SPECIAL TERMS AND CONDITIONS

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

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

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

From: _____

Name of Offeror Due Date Time

Street or Box No. RFP #

City, State, Zip Code RFP Title

Name of Purchasing Officer:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IX. METHOD OF PAYMENT

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

X. PRICING SCHEDULE

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

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

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

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

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

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

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

   Years_____ Months_____

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

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

_____

_____

_____

_____

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

_____

_____

_____

ATTACHMENT B

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

Offeror Name: _____ Preparer Name: _____

Date: _____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date: _____

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: _____ Date Form Completed:_____

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

Offeror / Proposer:

Firm	Address	Contact Person/No.
_____	_____	_____

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

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

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

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

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

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

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

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

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

ATTACHMENT D

Zone Map

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

List of member institutions by zones

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