JMU
JAMES MADISON
UNIVERSITY.

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU7140**

This contract entered into this 25th day of March 2025, by Anthony Timbers, 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 1, 2025 through March 30, 2026 with nine (9) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

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

(3) The Contractor's Proposal dated January 28, 2025 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
  (a) Negotiations Summary, dated March 17, 2025.

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

CONTRACTOR:	PURCHASING AGENCY:
By: ______________	By: ______________
(Signature)	(Signature)
Anthony Timbers	Doug Chester
(Printed Name)	(Printed Name)
Title: CEO	Title: Buyer Senior

JAMES MADISON UNIVERSITY

RFP # FDC-1220
Information Technology Security Auditing Services
Negotiation Summary for Anthony Timbers, LLC.
March 17, 2025

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

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

3. The pricing schedule is as follows:

Pricing for Auditing Services	Off-site	On-site*
External Vulnerability Scanning	125.04	135.04
Wireless Network Assessment	125.04	135.04
Firewall and Router Security Assessment	125.04	135.04
Server Configurations Assessment	125.04	135.04
Database Architecture Security Assessment	125.04	135.04
Network Scanning Process Assessment	125.04	135.04
Web Application Security Assessment	125.04	135.04
Active Directory Security Assessment	125.04	135.04
Penetration Testing	125.04	135.04
Telecommunications	125.04	135.04
* (flat fee hourly rate that includes all billables/travel)		

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

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

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

REQUEST FOR PROPOSAL

RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

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

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

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

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

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

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

Name and Address of Firm:
Anthony Timbers LLC

By: Anthony Timbers
(Signature)

Name: Anthony Timbers
(Please Print)

Date: 01/28/2025

Title: CEO

Web Address: https://anthonytimbers.com

Phone: 804-596-0596

Email: a.timbers@anthonytimbers.com

Fax #: NA

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 ADT #2 ADT #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.

James Madison University
IT Security Auditing Services RFP
RFP# FDC-1220

Due Date: January 30th, 2025

JMU
JAMES MADISON
UNIVERSITY

ANTHONY TIMBERS
PROTECT YOUR COMPANY WITH A CYBERSECURITY PLAN

Submitted by:
Anthony Timbers LLC
1320 Central Park Blvd Suite 200
Fredericksburg, VA 22401

Point of Contact:
Anthony Timbers
(202) 731-9376
a.timbers@anthonytimbers.com

Submitted to:
James Madison University
Procurement

TABLE OF CONTENTS

Company Executive Summary 3
- Company Overview 3
- Differentiators 3
- ISO 17020:2012 Accredited Cybersecurity Inspection Body 4
- Past Performance 6
- Public Sector Past Performance 6
  - Public Sector Past Performance – 1 6
  - Public Sector Past Performance – 2 7
  - Public Sector Past Performance – 3 7
  - Public Sector Past Performance – 4 7
  - Public Sector Past Performance – 5 8
  - Public Sector Past Performance – 5 8
  - Public Sector Past Performance – 6 8
  - Public Sector Past Performance – 7 9
  - Public Sector Past Performance – 8 9
  - Public Sector Past Performance – 9 9
  - Public Sector Past Performance – 10 10
  - Public Sector Past Performance –11 10
  - Public Sector Past Performance – 12 10
  - Public Sector Past Performance – 13 11
  - Public Sector Past Performance – 14 11
  - Public Sector Past Performance – 15 11
  - Public Sector Past Performance – 16 12
- Private Sector Past Performance 12
  - Private Sector Past Performance – 1 12
  - Private Sector Past Performance – 2 13
  - Private Sector Past Performance – 3 13
  - Private Sector Past Performance – 4 13
  - Private Sector Past Performance – 5 14
  - Private Sector Past Performance – 6 14

- history in working with institutions of higher education 15
- Proposer Capabilities 15
  - Professional Summaries 15
  - Key Personnel Qualification Overview/Resumes 17
  - Procedures for if Key Personnel No Longer Available 18

Project Approach 18

- Project Management 18
- Communications Management Plan 19
- Quality Assurance Plan 20
- External Vulnerability Scanning 20
- Network Scanning Process Assessment 21
- Telecommunications 21
- Server Configurations Assessment 22
- Firewall and Router Security Assessment 22
- Database Architecture Security Assessment 23
- External/Internal/Active Directory Penetration testing Methodology 24
- Web Application Penetration Testing and Security Assessment Methodology 28
- Wireless Network Assessment 30
- Cloud Security Assessment 31
- Testing Location Methodology 31
- Tools to Be Utilized for Penetration Testing 31

Secure Collaboration Solution 32

Anthony Timbers LLC Data Security 32

COMPANY EXECUTIVE SUMMARY

Company Overview

A brief profile of the firm can be found below:

Table 1: Company Details

Company Name	Anthony Timbers, LLC		
Business Structure	Limited Liability Company (LLC)		
Business Size	Small (9 Employees)	Number of Locations	1
Principal Place of Business	1320 Central Park Blvd Suite 200 Fredericksburg, VA 22401 (Location Services to be Provided From)		
Date of Organization	January 12th, 2020	Length of Time in Business	5 Years
Business Certifications	**SWaM Certified Business** (*Small, Minority-Owned Business, Certification #814873*) **PCI-DSS Qualified Security Assessor** **ISO 17010:2012, Certified Cybersecurity Inspection Body** (*Certification #7270.01*) **CMMC Certified Third Party Assessment Organization** (C3PAO)		
Contract Vehicles	GSA IT Schedule 70 (54151HACS) *Contract #47QTCA21D00BS*		
DUNS	117336232	CAGE Code	8FKE0
Federal EIN	[redacted]		

Differentiators

Some key points that separate Anthony Timbers LLC from other companies that may bid on this engagement are:

- We are an **authorized CMMC C3PAO**, showing our expertise in the field of conducting NIST 800-171 assessments
- We provide cybersecurity professionals with a minimum of a Security+ and CEH/Pentest+/OSCP (or equivalent) for red team engagements and bring high experience web application penetration testers to this engagement
- Our staff has conducted hundreds of penetration tests, including tests on large county networks with numerous departments and over 10,000+ devices
- We are **ISO 17020:2012 certified**, ensuring rigorous standards for our inspection services, with an accreditation scope that includes Penetration Testing, enhancing our capability to deliver superior penetration testing services.
- We bring 50+ years of experience conducting cybersecurity engagements for both commercial and governmental entities
- We produce quality deliverables by utilizing a Quality Management System (QMS) based on ISO 9001 for every project we undertake

One other thing that sets us apart from many other companies that may bid on this opportunity and shows our qualification and experience more is that not only are we a ***GSA IT Schedule 70*** contract holder under the ***Highly Adaptive Cybersecurity Services (HACS)*** SIN, we are qualified **for each** HACS SIN category.

This means that we have gone through a rigorous vetting process and have proven our ability to perform the work required by this RFP and to have the experience/knowledge necessary to take on the following types of work:

1. High-Value Asset Assessments, to include Security Architecture Reviews and Systems Security Engineering
2. Risk and Vulnerability Assessments
3. Cyber Hunting
4. Incident Response
5. Penetration Testing

ISO 17020:2012 Accredited Cybersecurity Inspection Body

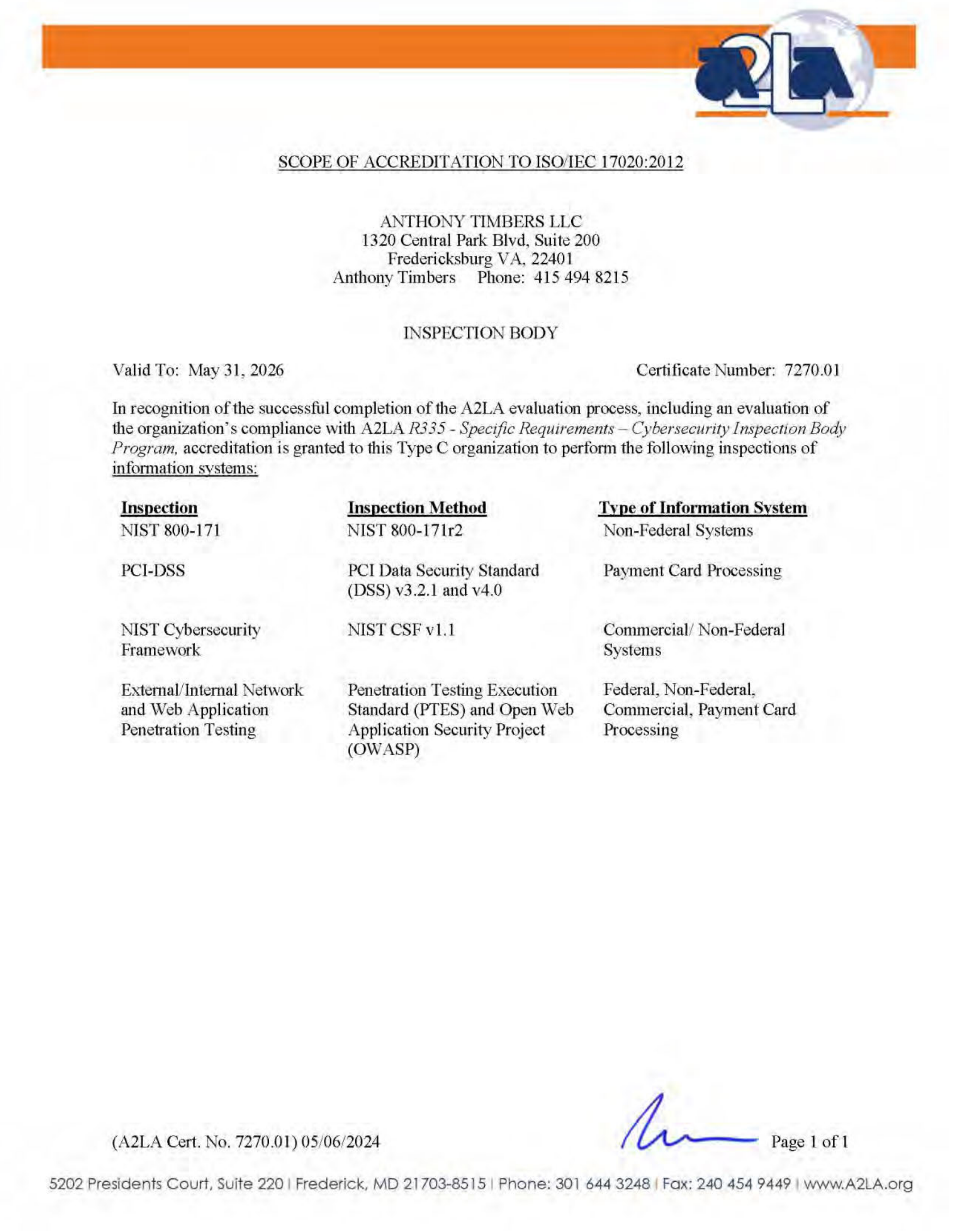
Anthony Timbers LLC brings a unique level of expertise and accreditation to the table for conducting the requested work. As an **ISO 17020:20212** certified inspection body and a participant in the **Cybersecurity Inspection Body Program**, audited by **A2LA**, our scope of accreditation includes:

- NIST 800-171,
- PCI-DSS 3.2.1 and 4.0,
- **External/Internal Network and Web Application Penetration Testing**
- NIST CSF

This accreditation signifies that we have undergone rigorous assessment and auditing processes, ensuring that our staff are highly qualified inspectors with in-depth knowledge and experience in cybersecurity standards and practices. Our accreditation in Penetration Testing highlights our ability to assess and validate the security posture of JMU and provides and serves as an independent audit report of our capabilities.

Being part of the Cybersecurity Inspection Body Program further emphasizes our commitment to maintaining the highest standards of quality and proficiency in cybersecurity assessments. Our staff, who have undergone accreditation with an auditor, possess the expertise and skills necessary to conduct thorough and reliable security assessments, making us uniquely qualified to handle the complexities of the requested work.

Our accreditation and experience are a significant advantage, demonstrating our capability to deliver comprehensive and effective cybersecurity assessments that meet regulatory requirements and industry best practices. This level of accreditation underscores our commitment to excellence and ensures that our clients receive reliable, trustworthy, and high-quality services.



SCOPE OF ACCREDITATION TO ISO/IEC 17020:2012

ANTHONY TIMBERS LLC
1320 Central Park Blvd, Suite 200
Fredericksburg VA, 22401
Anthony Timbers   Phone: 415 494 8215

INSPECTION BODY

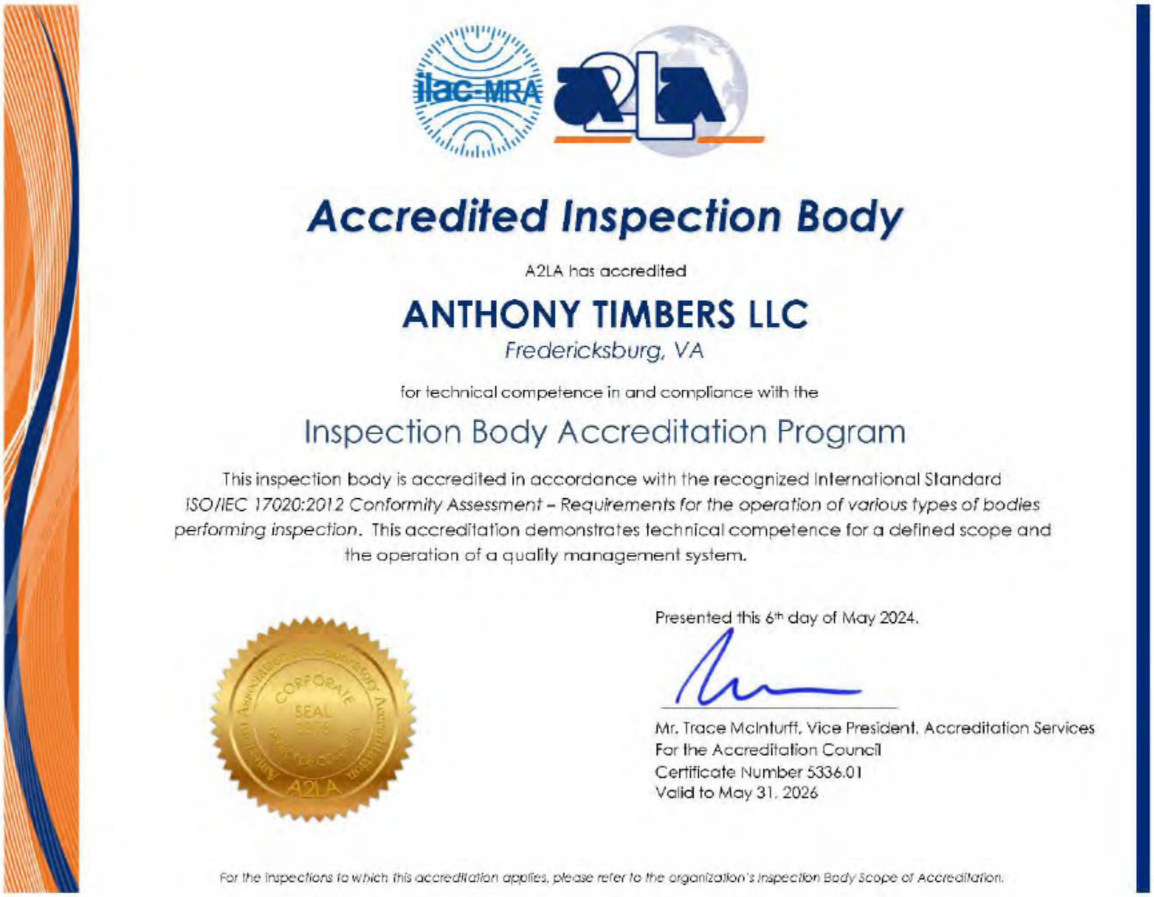
Valid To: May 31, 2026   Certificate Number: 7270.01

In recognition of the successful completion of the A2LA evaluation process, including an evaluation of the organization's compliance with A2LA *R335 - Specific Requirements – Cybersecurity Inspection Body Program,* accreditation is granted to this Type C organization to perform the following inspections of information systems:

Inspection	**Inspection Method**	**Type of Information System**
NIST 800-171	NIST 800-171r2	Non-Federal Systems
PCI-DSS	PCI Data Security Standard (DSS) v3.2.1 and v4.0	Payment Card Processing
NIST Cybersecurity Framework	NIST CSF v1.1	Commercial/ Non-Federal Systems
External/Internal Network and Web Application Penetration Testing	Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP)	Federal, Non-Federal, Commercial, Payment Card Processing

(A2LA Cert. No. 7270.01) 05/06/2024   Page 1 of 1

5202 Presidents Court, Suite 220 | Frederick, MD 21703-8515 | Phone: 301 644 3248 | Fax: 240 454 9449 | www.A2LA.org



Accredited Inspection Body

A2LA has accredited

ANTHONY TIMBERS LLC

Fredericksburg, VA

for technical competence in and compliance with the

Inspection Body Accreditation Program

This inspection body is accredited in accordance with the recognized International Standard *ISO/IEC 17020:2012 Conformity Assessment – Requirements for the operation of various types of bodies performing inspection*. This accreditation demonstrates technical competence for a defined scope and the operation of a quality management system.

CORPORATE SEAL
A2LA

Presented this 6th day of May 2024.

Mr. Trace McInturff, Vice President, Accreditation Services
For the Accreditation Council
Certificate Number 5336.01
Valid to May 31, 2026

For the inspections to which this accreditation applies, please refer to the organization's Inspection Body Scope of Accreditation.

Past Performance

Organizations in both the public and private sectors have entrusted Anthony Timbers LLC and other members of our project team to assist in proactively securing assets and minimize cybersecurity impact to business operations. Our experience includes conducting security assessments for large university systems, hospitals, government agencies, and large/small businesses. Below are some of the relevant experiences that qualify our company and the engagement team to provide superior cybersecurity services.

Public Sector Past Performance

Public Sector Past Performance – 1

Client		
City of Bakersfield, CA		
Type of Work	**Period of Performance**	**Place of Performance**
External/Internal Penetration Testing	September 2024- January 2025	Remote
Description		
We conducted a comprehensive penetration test for the City of Bakersfield, CA, encompassing over 5,000 external and internal addresses. The assessment included external and internal network penetration testing and vulnerability scanning, Wi-Fi penetration testing, and a detailed		

penetration test/assessment of the Active Directory environment. Our approach identified critical vulnerabilities and misconfigurations, providing actionable recommendations to enhance the client's overall security posture and safeguard their IT infrastructure.

Public Sector Past Performance – 2

Client		
Town of Palm Beach, FL		
Type of Work	**Period of Performance**	**Place of Performance**
External/Internal Penetration Testing	August 2024 – September 2024	Remote
Description		
We conducted penetration test for the Town of Palm Beach, FL, encompassing approximately 13 /24 subnets internally and various domains and a /26 network externally. The assessment included external and internal network penetration testing and vulnerability scanning, Wi-Fi penetration testing, and a penetration test/assessment of the Active Directory environment.		

Public Sector Past Performance – 3

Client		
City of Palm Beach Gardens, FL		
Type of Work	**Period of Performance**	**Place of Performance**
Penetration Testing, Web Application Vulnerability Scanning, CIS v8 Assessment	June 2024 – August 2024	Remote
Description		
External and internal penetration test of the City's network and web applications. Also providing a full CIS v8 assessment on the City to determine their compliance with the CIS controls.		

Public Sector Past Performance – 4

Client		
US Marine Corps		
Type of Work	**Period of Performance**	**Place of Performance**
External/Internal/Web Application PCI-DSS Penetration Testing and Targeted Risk Analysis	June 2024 - Present	Remote and On-Site
Description		
Currently on a 5-year contract with the Marine Corps to provide annual External/Internal PCI-DSS Penetration Testing Services for their large CDE network well as providing Annual Targeted Risk Analysis services in support of PCI-DSS 4.0 compliance.		

Public Sector Past Performance – 5

Client		
Maricopa County		
Type of Work	**Period of Performance**	**Place of Performance**
Penetration Testing, Cybersecurity Consulting	December 2022- Present	Remote/Onsite
Description		
Providing Penetration testing services to the county and all of Arizona, to include Internal, External, Web Application, and other forms of penetration testing. General Cybersecurity Consulting is also provided under this contract. Currently, we have conducted numerous web application penetration tests for highly critical county systems/applications and provided tremendous value by identifying various vulnerabilities for them to remediate.		

Public Sector Past Performance – 5

Client		
Hawaii Department of Business, Economic Development & Tourism		
Type of Work	**Period of Performance**	**Place of Performance**
External/Internal Penetration Testing	August 2024 - Present	Remote
Description		
As part of the Hawaii Cyber Safe Program, we are conducting penetration testing for up to 40 small businesses to enhance their cybersecurity resilience. To date, we have been assigned approximately 10 businesses, performing tailored assessments that include external and internal penetration testing, vulnerability scanning, and network security evaluations. Our work helps small businesses identify and mitigate security risks, empowering them to protect sensitive data and maintain compliance with industry standards.		

Public Sector Past Performance – 6

Client		
State of New Hampshire Employment Security		
Type of Work	**Period of Performance**	**Place of Performance**
PCI-DSS Forensics Investigations, Penetration Testing	October 2024 – November 2024	Remote
Description		
Provided extensive forensics investigation services and penetration testing services after a breach was reported for the NHES. We did a deep, thorough investigation of logs and activity and provided an actionable report. We also conducted a penetration test to see if the environment		

and web application was still at-risk post incident. We have an ongoing agreement to conduct quarterly penetration testing with this unit as well.

Public Sector Past Performance – 7

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">State of New Hampshire</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>PCI-DSS Forensics Investigations</td><td>February 2024 – Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We currently provide comprehensive PCI DSS forensic investigation services to various state agencies upon request, leveraging advanced forensic techniques to assess and enhance their payment system security. Our expert team conducts detailed analyses to identify compliance gaps and vulnerabilities, ensuring adherence to the highest standards of data protection. Through our specialized incident response and training programs, we empower agencies to effectively safeguard sensitive cardholder information against potential breaches and fraud.</td></tr>
</table>

Public Sector Past Performance – 8

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">CA Department of Parks and Recreation</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>PCI-DSS ASV Scanning and Penetration Testing</td><td>May 2023 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We are currently providing PCI-DSS vulnerability scanning quarterly and penetration testing as required in support of the department's PCI-DSS compliance efforts for 300+ locations. We will be using an ASV solution (Tenable.io) for scanning and conducting network and web application penetration tests on in scope-environments for 16 months.</td></tr>
</table>

Public Sector Past Performance – 9

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">City of St. Charles, IL</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>Managed Cybersecurity Services, PCI-DSS Penetration Testing/ASV Scanning, Vulnerability Scanning and Program Management, General Network Penetration Testing</td><td>June 2023 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We are providing full managed cybersecurity services for the entire city. This includes SIEM implementation/monitoring, vulnerability management, annual risk assessments,</td></tr>
</table>

network/application penetration tests (1,000+ devices), 24x7 network monitoring, incident response services, and other cybersecurity consulting engagements as needed. PCI-DSS ASV scanning and penetration testing is also handled/managed by our team.

Public Sector Past Performance – 10

Client		
Suffolk County, New York		
Type of Work	**Period of Performance**	**Place of Performance**
NIST CSF Assessment, External/Internal/Web Application Penetration Test	September 2023 - February	Remote
Description		
In our role as a third-party provider, we conducted a thorough External/Internal/Web Application Penetration Test as part of the city's NIST CSF Assessment. Our expert team meticulously assessed the security of the city's systems and web applications, identifying vulnerabilities and potential risks on a network of 10,000+ devices. By delivering actionable insights and recommendations, we assisted the city in enhancing its cybersecurity defenses and fortifying its infrastructure, thereby safeguarding sensitive information and ensuring compliance with NIST Cybersecurity Framework standards.		

Public Sector Past Performance –11

Client		
Massachusetts Office of the State Auditor		
Type of Work	**Period of Performance**	**Place of Performance**
Cybersecurity Architecting, Cybersecurity Consulting, Compliance Assessment/Implementation	July 2022 – Present	Remote
Description		
We are currently performing on a contract as the Information Security Architect for the Massachusetts Office of the State Auditor. Our job includes conducting an initial cybersecurity assessment on the network as a whole and documenting compliance with applicable NIST/CIS controls. We are providing ongoing cybersecurity architecting services, which includes conducting risk assessments, architecting a more secure environment, building out a formalized security program, implementing security controls and tools, creating and formalizing security policies/procedures, assisting with migration to Office 365 cloud, securing the cloud O365 tenant, hardening network devices and servers, and making overall recommendations to improve their security posture.		

Public Sector Past Performance – 12

Client
Ohio University

<table>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>NIST 800-171 Consulting, Cybersecurity Consulting</td><td>February 2023 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We are currently performing on a contract with Ohio University to provide CMMC training, consulting, and readiness/gap assessments for Ohio small businesses. Work includes determining scope of CMMC compliance for each business (Level 1 vs Level 2), assessing compliance with each control, and providing remediation details and recommendations to improve their compliance and cybersecurity overall. To date, we have completed 50+ NIST 800-171 gap assessments.</td></tr>
</table>

Public Sector Past Performance – 13

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">Virginia Retirement System</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>Cybersecurity Consulting, Penetration Testing</td><td>May 2023 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">Providing various cybersecurity services, primarily based around penetration testing and cybersecurity/compliance assessments to agencies in VA. Since it is a cooperative purchasing agreement, VA agencies can utilize the contract for cybersecurity consulting as needed via eVA.</td></tr>
</table>

Public Sector Past Performance – 14

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">San Joaquin County Government</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>Cybersecurity Consulting, Compliance Assessment, Zero Trust Architecting</td><td>October 2021 – June 2022</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We are working on a contract with the San Joaquin County Sherriff's Department to conduct both a cybersecurity assessment of their network and implement the Microsoft Zero Trust Strategy for their 365 environments. We have completed the initial cybersecurity posture assessment and are currently implementing various Zero Trust features for them. In this effort, we conducted an assessment and determined the current levels of risk that they face, where their cybersecurity gaps currently are, and providing recommendations on how they can improve their cybersecurity overall. This included assessing compliance with NIST 800-171/CMMC as well.</td></tr>
</table>

Public Sector Past Performance – 15

<table>
<tr><th>Client</th></tr>
<tr><td>GENEDGE</td></tr>
</table>

Type of Work	Period of Performance	Place of Performance
Cybersecurity Consulting, CMMC Compliance, Managed Security Services, Vulnerability/Risk Assessments	May 2021 – Present	Remote
Description		
We work directly with GENEDGE on implementing remediation actions for clients that need to be CMMC compliant. We typically implement all the NIST 800-171 controls for their secure enclaves that we build out and act as their Managed Security Service provider if requested and continually manage their security program, which includes conducting vulnerability assessments weekly, patch management, conducting SIEM monitoring, conducting Incident Response, and managing other security tools we deploy. An initial assessment is done on the organizations we work with to determine what needs to be implemented. We provide our recommendations and gameplan for improving their cybersecurity posture.		

Public Sector Past Performance – 16

Client		
NJ Transit		
Type of Work	**Period of Performance**	**Place of Performance**
PCI-DSS Audit/Assessment, PCI 4.0 Gap Assessment and Audit	November 2023 - Present	Remote and On-Site
Description		
We currently support NJ Transit, a level 1 merchant, on a 3 year contract conducting PCI-DSS assessments for them as Qualified Security Assessors (QSAs). We completed a full Level 1 audit and assessment of their PCI-DSS compliance and completed a RoC/AoC for them and will be conducting this for the next 3 years, including mandatory on-site visits for parts of the assessment each year. A gap analysis from PCI-DSS v3.2.1 to v4 is also being conducted. A review of all their cybersecurity practices for their in-scope environment was completed and recommendations/remediations for deficiencies were provided.		

Private Sector Past Performance

Private Sector Past Performance – 1

Client		
Janus Logistics Technologies		
Type of Work	**Period of Performance**	**Place of Performance**
Penetration Testing	June 2024 - Present	Remote
Description		
We are conducting a penetration test on an application and its infrastructure or a small business, Janus Logistics Technologies.		

Private Sector Past Performance – 2

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">Multistate Partnership for Prevention</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>Cybersecurity Consulting, HIPAA/NIST Compliance, Penetration Testing, Vulnerability/Risk Assessments</td><td>July 2020- May 2021</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">Managed Cybersecurity & HIPAA Compliance effort for a nationally used healthcare application known as PrepMod. We were brought in to do a security assessment of the application and their organization and to make recommendations on how to improve the security posture of each, followed by actually implementing them. Duties included conducting risk assessments, network/web application penetration testing, source code analysis, vulnerability assessments, application security implementation, AWS security management, cybersecurity consulting and engineering, and HIPAA compliance implementation/management.</td></tr>
</table>

Private Sector Past Performance – 3

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">Polimaster Inc.</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>Cybersecurity Consulting, CMMC Compliance, Managed Security Services, Vulnerability/Risk Assessments</td><td>December 2021 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">We worked directly with Polimaster Inc., a DoD contractor, on implementing a secure CMMC enclave in Office 365 and making recommendations to formalize and improve their security program. We provided cybersecurity consulting services and implemented all the NIST 800-171 controls for their secure enclave. We now act as their Managed Security Service provider and continually manage their security program, which includes conducting vulnerability assessments weekly, conducting SIEM monitoring, conducting Incident Response, and managing the XDR tool we deployed for them.</td></tr>
</table>

Private Sector Past Performance – 4

<table>
<tr><th colspan="3">Client</th></tr>
<tr><td colspan="3">Cino Security Solutions</td></tr>
<tr><th>Type of Work</th><th>Period of Performance</th><th>Place of Performance</th></tr>
<tr><td>External Penetration Testing and Vulnerability scanning</td><td>February 2020 - Present</td><td>Remote</td></tr>
<tr><th colspan="3">Description</th></tr>
</table>

External Penetration Testing for a large number of clients using public IP addresses. Testing covers network and website/web app penetration testing. We went/go through a robust external penetration testing methodology that includes conducting reconnaissance, port scanning, vulnerability scanning, and enumerating vulnerabilities using a number of penetration testing tools. The overall goal is to gain some type of access to the network or device from the outside, which we have achieved on multiple occasions. A penetration testing report is generated after each engagement that contains all steps taken and detailed remediation actions to take. All testing is 100% blackbox. We make recommendations to clients on how they can improve their cybersecurity posture based on our findings.

Private Sector Past Performance – 5

Client		
Immigrant Legal Resource Center		
Type of Work	**Period of Performance**	**Place of Performance**
External/Internal Vulnerability Scanning and Penetration Testing	July 2020 - August 2020	Remote
Description		
Internal and External security assessment of infrastructure and corporate networks (100+ devices). The external portion of this assessment included penetration testing and vulnerability scanning multiple websites/web applications, as well as the edge devices of the network (firewalls/routers). Internally, we conducted penetration testing on the active directory domain and looked for exploitable vulnerabilities in servers and workstations. Vulnerability scanning was conducted internally as well to detect potential vulnerabilities in systems on the network. We made recommendations to the organization on how to improve their cybersecurity posture based on the findings from our assessment.		

Private Sector Past Performance – 6

Client		
Skysoft Inc.		
Type of Work	**Period of Performance**	**Place of Performance**
Web Application, External, and Internal Penetration Testing and Vulnerability Assessments	January 2020 – Present	Remote
Description		
Internal and External Penetration Testing of infrastructure and corporate networks (200+ devices). While on the internal network of a healthcare organization, we stepped through our penetration testing methodology in order to discover any potentially exploitable vulnerabilities. Vulnerability scanning and testing of the Active directory domain were in scope for this assessment as well. We also conduct web application penetration testing on healthcare applications that require HIPAA compliance. We conducted a number of automated and manual tactics in order to uncover a number of vulnerabilities in the deployed healthcare application. The testing was Blackbox testing primarily, as well as some testing using credentials for the web application and vulnerability scans separately.		

HISTORY IN WORKING WITH INSTITUTIONS OF HIGHER EDUCATION

Anthony Timbers LLC has extensive experience working with institutions of higher education, including those within the Commonwealth of Virginia and beyond. Our firm has partnered with Ohio University and the Ohio Apex Accelerator to provide cybersecurity consulting and CMMC compliance services, supporting over 35 small businesses in Ohio.

Additionally, we worked with Johnson County Community College (JCCC) in Kansas to develop a custom cybersecurity awareness web application tailored for small businesses. This initiative included creating multiple hours of cybersecurity awareness training content, including instructional videos, to enhance security education for small business owners and employees.

Our expertise spans cybersecurity consulting, compliance assessments, penetration testing, and security awareness training, making us well-equipped to support institutions of higher education in Virginia. Whether through security assessments, compliance readiness, or custom security awareness programs, we bring a deep understanding of cybersecurity best practices and regulatory frameworks such as CMMC, NIST 800-171, and PCI DSS to educational institutions and their partners.

PROPOSER CAPABILITIES

Professional Summaries

One of our lead cybersecurity consultants for this engagement will be ***Anthony Timbers***. ***Anthony Timbers*** is a ***Cybersecurity Expert and Certified Ethical Hacker (CEH)*** with ove***r 12 years of experience***. He has a large amount of experience working with both governmental and non-governmental entities on various cybersecurity engagements, including penetration tests (internal and external with up to 10,000+ hosts and web applications), vulnerability assessments (environments with well over 4000+ hosts), risk assessments, cybersecurity implementations, PCI-DSS/HIPAA/NIST compliance consulting, general consulting, and more. He has completed 100+ cybersecurity engagements, including PCI-DSS Level 1 Audits, and can leverage that experience to provide JMU with top-notch cybersecurity services. He will be acting as the lead consultant for the engagement and will be one of the lead pen testers for JMU.

Mr. Timbers currently holds a ***master's degree in Cybersecurity and Information Assurance***, along with several industry-standard cybersecurity certifications, including:

- Certified Ethical Hacker Certificate (***CEH***)
- Computer Hacking Forensic Investigator (***CHFI***)
- PCI-DSS Qualified Security Assessor (**QSA**)
- Certified Information Systems Security Professional (***CISSP***)
- Certified Information Systems Auditor (***CISA***)
- CompTIA **Security+, CySA+,** and **Cloud+**
- NIST Cybersecurity Framework Professional Practitioner (***NCSP***)

Next, we have ***Khalil Hicks***, an ***expert level cybersecurity expert*** with over 10 years of experience as well conducting penetration testing on large networks. Mr. Hicks has experience as a principal engineer performing both offensive and defensive cybersecurity operations including SOC monitoring, network/web application penetration testing, vulnerability scanning, incident response, device configuration reviews, and other security related activities that relate to this engagement. **Mr. Hicks** currently holds a ***master's degree in Cyber Operations***, along with several industry-standard cybersecurity/networking certifications, including:

- Certified Information Systems Security Professional (***CISSP***)

- Offensive Security Certified Professional (**OSCP**)
- Certified Red Team Operator
- eWPT - eLearnSecurity Web Application Penetration Tester
- eCPPT – eLearnSecurity Certified Professional Penetration Tester
- GIAC Certified Incident Handler (**GCIH**)
- GIAC Certified Forensics Analyst (**GCFA**)
- NIST Cybersecurity Framework Professional Practitioner (***NCSP***)

Next, we have ***Ashley Hall*** brings over six years of experience in cybersecurity, with a primary focus on penetration testing and vulnerability assessment across diverse client environments. She has led and executed internal and external penetration testing engagements, delivering actionable insights to both technical teams and executive leadership. Holding certifications such as GIAC Certified Incident Handler (GCIH), **Practical Network Penetration Tester (PNPT)**, **Certified Ethical Hacker (CEH)**, and CompTIA Security+, Ashley is proficient in leveraging tools like Metasploit, Burp Suite, and Nmap to uncover and address critical vulnerabilities. Her expertise, combined with hands-on technical skills and a commitment to excellence, makes her a highly qualified professional in the field of penetration testing.

Next, we have ***Nicole Moran***, a ***junior cybersecurity specialist*** with over 3 years of experience in the field. Currently, she serves as a valuable member of the Anthony Timbers LLC team, where she has made significant contributions for the past three years. Nicole is a **CompTIA *Security*+ and Pentest+** certified professional, demonstrating her commitment to excellence in the field of penetration testing. She has played a pivotal role in various cybersecurity projects, showcasing her expertise in vulnerability management and penetration testing on public sector client networks. With her dedication and knowledge, Nicole continues to enhance the security posture of organizations she collaborates with, making her an indispensable asset in the cybersecurity realm. Nicole will play a crucial support role during vulnerability scanning and analysis, leveraging her experience and expertise to assist in identifying and rooting out false positives, ensuring that security efforts remain focused on genuine threats.

Next we have ***Isaac Nkaada***, a ***Cybersecurity and audit expert with 7 years of experience***. Isaac Nkaada is a distinguished cybersecurity consultant at Anthony Timbers LLC, specializing in PCI DSS compliance, CMMC Compliance, and NIST based audits. Isaac is a **CMMC CCP/CCA**, **PCI-DSS QSA**, **CISM**, **CISA**, and **CompTIA Security+** certified professional, reinforcing his deep-rooted knowledge in information systems management and auditing, as well as PCI-DSS and NIST frameworks. His expertise is the product of a rich career that includes a significant tenure as an auditor at Ernst & Young, where he cultivated a keen understanding of industry security frameworks. His hands-on experience spans across high-profile clients such as New Jersey Transit, the Marine Corps, FCB Bank, Starbucks Call Center, and Caterpillar Mobile App, each requiring unique solutions and services for their Cybersecurity and PCI DSS compliance needs.

The final key personnel we plan to have on this assignment is our Senior Project Manager, ***Edwin Johnson***. Edwin Johnson is ***PMP certified*** and has 10 years of experience in project management through his experience working with the Department of Homeland Security and Anthony Timbers LLC. He has worked across a range of projects from the modernization of government systems to national security-related projects, and the migration of data to cloud environments. He has successfully managed and completed a project on a $10M IT-related contract. His goal with every project is to ensure that his client receives a product that they are satisfied with and that directly matches their business needs. Mr. Johnson has led several projects for cybersecurity consulting during his time with our firm and brings his project management expertise to this engagement.

It is worth noting that we have a number of other qualified personnel that we can dedicate to this effort as well depending on the load.

Key Personnel Qualification Overview/Resumes

Team Member	Years of Cybersecurity Experience	Education	Relevant Certifications
Anthony Timbers, Senior Cybersecurity Consultant	12+ Years	M.S., Cybersecurity and Information Assurance	Certified CMMC Professional (CCP) Certified CMMC Assessor (CCA) CISA CISSP CEH CHFI Security+ CySA+ Cloud+ PCI-DSS QSA NIST Cybersecurity Framework Professional Practitioner (NCSP)
Khalil Hicks, Senior Cybersecurity Consultant	12+ Years	M.S., Cyber Operations	CISSP OSCP Certified Red Team Operator eWPT - eLearnSecurity Web Application Penetration Tester eCPPT – eLearnSecurity Certified Professional Penetration Tester GCIH GCFA NIST Cybersecurity Framework Professional Practitioner (NCSP)
Ashley Hall, Junior Penetration Tester	12+ Years	BS in Computer Science: Information Assurance	GCIH PNPT CEH GCFE, CompTIA Security+ CompTIA Network+
Nicole Moran, Junior Cybersecurity Consultant	3+ Years	B.A in Media Arts and Design	Security+ Pentest+
Isaac Nkaada, Senior	7+ Years	B.S., Cybersecurity Management and Policy	Certified CMMC Professional (CCP)

Cybersecurity Consultant			Certified CMMC Assessor (CCA) (Pending) CISA CISM Security+ PCI-DSS QSA
Edwin Johnson, Senior Project Manager	10+ Years	B.S. in Criminal Justice, Minor in Intelligence Analysis M.S. in Information Technology, Concentration: Homeland Security Management	PMP PMI Agile Certified Practitioner

Procedures for if Key Personnel No Longer Available

We understand the importance of maintaining consistency and transparency in project staffing. To ensure seamless project continuity and effective communication, we have established comprehensive procedures for managing changes in project personnel. Below, we outline our approach and steps to notify JMU about any changes in staffing:

1. **Immediate Notification:** When a team member is no longer assigned to the project or leaves our company, the immediate supervisor will inform our Human Resources (HR) department and project manager without delay. This prompt action ensures that we can quickly initiate the process of identifying a suitable replacement.
2. **Utilizing Our Talent Pool:** Our organization maintains a pool of highly skilled professionals and a robust network within the cybersecurity industry. This enables us to rapidly identify and deploy a qualified replacement to minimize any disruption to the project. Our talent pool includes experts in MSSP services, monitoring, pen testing, vulnerability assessments, and consulting engagements.
3. **Selection and Assignment:** HR, in collaboration with the project manager, will select a replacement from our internal talent pool or external network. The selected candidate will possess the necessary qualifications and experience to seamlessly continue the project tasks.
4. **Transfer of Knowledge and Responsibilities:** The departing team member, where possible, will document all current tasks, status updates, and critical project information. This documentation will be handed over to the replacement personnel. Additionally, the new team member will undergo a rapid orientation and training session to ensure they are fully prepared to take over the responsibilities immediately.

PROJECT APPROACH

PROJECT MANAGEMENT

When leading and managing projects, Anthony Timbers LLC typically takes the following approach:

1. Initiation
    a) Creating a project initiation document
    b) Defining objective, purpose and discussing deliverables for the proposed project
    c) Identifying potential risks and constraints
    d) Secure funding for the project, if necessary

   e) Review the budget to determine the timeline and cost needed to complete the project
   f) Building a team based on complexity and need for the project – defining roles and responsibilities

2. Planning – Using the smart method (specific, measurable, attainable, realistic & timely)
   a) Establish the goals
   b) Decide how the goals will be measured
   c) Identify priorities and establish deadlines
   d) Distinguish assignments & accountability
   e) Create the timeline – including the scope of the project, milestones, communication plan and risk/prevention plan.
3. Execution
   a) Initiating the project
   b) Assigning resources
   c) Implementing a project management plan
4. Monitor & Control
   a) Amending project plans as needed
   b) Updating project schedule
   c) Communicating changes with the team
   d) Reviewing project objective and cost tracking
   e) Addressing any issues that may arise
5. Project Completion
   a) Manage project until completion

Our project manager who will be overseeing these engagements is Edwin Johnson. Mr. Johnson is one of our Senior Project Managers and will be assigned to the role of managing the assessments of these small businesses. More information on Mr. Johnson and other proposed team members can be found in a later section of the proposal.

Communications Management Plan

During these projects, communication will be important. To provide the highest quality solution and support, we propose the following plan for communications:

Communication Plan

Type of Communication	Objective	Format	Frequency	Audience	Deliverable
Weekly status meeting	To discuss project status/ identify potential risks	Virtual	Weekly	Project team Stakeholders	Agenda
Team status meeting	To internally discuss project status and to address any potential risks/concerns	Virtual	Weekly	Project team	Meeting minutes Agenda

Action items and follow-ups	To address requests from clients/stakeholders	Virtual	As needed	Project team Stakeholders	Agenda

Our plan is to have weekly status meetings as needed to ensure that you remain up to date with the status of the project and to discuss any risks. Internally, we will be meeting weekly to ensure that work is being completed and the project is still on the planned schedule. As needed, extra meetings for specific action items will be held to ensure all requests from JMU are addressed/resolved. This is to provide maximum levels of support as needed.

Quality Assurance Plan

The Anthony Timbers LLC Team has developed a proactive quality assurance feedback process to measure and report employee and client satisfaction. During the initial rollout, the Project Manager will contact the assigned staff when reporting to the assignment on the first day of work. Once the staff completes training, the Project Manager and/or a member of the management support team will contact both JMU representatives and the employees weekly via telephone or email to monitor employee performance and contract progress. Face-to-face meetings with a JMU-designated representative(s) are held as requested, to evaluate and review the development of the contract and address any concerns. The Anthony Timbers LLC Team performs the activities listed below to support our quality assurance program:

- **Performance Monitoring:** The Project Manager monitors performance metrics and contract deliverables to make sure that all tasks are completed
- **Status Reports:** Submit status reports to ensure accuracy and monitor project status
- **Call-Backs:** Perform call-backs on customer issues and concerns to make sure that all items are addressed appropriately
- **Cross-Training;** Assign personnel with different levels of expertise to the same task to ensure that personnel receive the job-cross training
- **Customer Feedback:** Solicit JMU feedback to improve procedures based on JMU suggestions
- **Staff Meetings:** Team members meet with the PM to be informed of current priorities and activities for the customer and within the Anthony Timbers LLC Team
- **Customer Meetings:** The Project Manager and staff attend meetings scheduled with JMU staff to gain insight into customer service and technical issues

While the Anthony Timbers LLC Team uses a very proactive approach, in dealing with people and services staff, personnel issues are inevitable. As these issues arise, they are addressed and dealt with in a timely manner. The Anthony Timbers LLC Team has received extensive training in coaching and counseling techniques, dispute resolution, and problem-solving. Anthony Timbers LLC Team’s Project Manager is available 24/7 to handle any emergency situations.

External Vulnerability Scanning

Our External Vulnerability Scanning process follows a structured methodology to assess externally facing assets for security vulnerabilities. The process begins with a kickoff meeting to define the scope of the engagement, identify all externally accessible IP addresses, and gather key information about the environment. During this phase, we ensure that all relevant stakeholders are aligned on the Rules of Engagement (RoE), including scan timing, impact mitigation strategies, and communication protocols.

Once the scope is finalized, we draft the Rules of Engagement (RoE) to outline the assessment parameters, ensuring compliance with industry best practices and client-specific requirements. With RoE approval, we conduct external vulnerability scans using Tenable Nessus, a leading vulnerability scanning solution. The scans evaluate externally accessible assets against known vulnerabilities, including Common Vulnerabilities and Exposures (CVEs), misconfigurations, and missing patches.

Following the scan, we analyze the results and generate a comprehensive report using our internal report generation system, PlexTrac. The report provides a detailed breakdown of discovered vulnerabilities, risk ratings, and remediation recommendations. We then conduct a stakeholder meeting to review the findings, ensuring that key personnel understand the risks and recommended mitigation strategies.

To ensure effective remediation, we provide technical guidance on mitigating identified vulnerabilities. Once remediation is complete, we conduct a follow-up scan to validate that vulnerabilities have been addressed, reducing the organization's external attack surface.

NETWORK SCANNING PROCESS ASSESSMENT

Our assessment of the current network scanning process begins with stakeholder interviews and documentation review to understand the organization's current approach, including:

- Scanning frequency (e.g., continuous, monthly, quarterly)
- Scope of scans (e.g., internal, external, cloud, OT/ICS environments)
- Scanning tools used (e.g., Tenable Nessus, Qualys, Rapid7, OpenVAS)
- Remediation workflows (e.g., how vulnerabilities are tracked, assigned, and mitigated)
- Integration with other security processes (e.g., SIEM, asset management)

Next, we benchmark the organization's scanning approach against industry standards and best practices to identify gaps and areas for enhancement. This includes assessing whether the organization:

- Conducts scans at an appropriate frequency based on risk level and compliance needs
- Scans all critical assets and network segments
- Properly validates and prioritizes vulnerabilities for remediation
- Implements an effective remediation and verification process

Following the assessment, we provide a detailed report with actionable recommendations, including enhancements to scanning frequency, tool selection, remediation processes, and reporting workflows. We also offer guidance on automating network scanning and integrating it into a continuous monitoring program to strengthen security posture.

TELECOMMUNICATIONS

When conducting a Telecommunications Security Audit, we will assess the security posture of JMUs telecommunications infrastructure, including VoIP systems, mobile networks, and supporting IT infrastructure. Our goal is to identify misconfigurations, vulnerabilities, and security gaps that could lead to unauthorized access, eavesdropping, service disruptions, or compliance violations.

We begin by reviewing the organization's telecommunications environment, which includes:

- VoIP and IP telephony systems
- Mobile device management (MDM) solutions and policies
- Wireless network configurations, including encryption and authentication
- Session Border Controllers (SBCs), firewalls, and security gateways
- Third-party telecom service providers and their security practices

We then conduct technical security testing, where we will:

- Assess VoIP security for risks such as SIP enumeration, call hijacking, and RTP interception
- Evaluate encryption and authentication mechanisms for weaknesses
- Review firewall configurations and access control policies to ensure protection against unauthorized access

- Test for Denial-of-Service (DoS) vulnerabilities and telephony spam (SPIT) risks

Upon completion, we will provide a detailed report outlining risks, vulnerabilities, and misconfigurations. Our report will include prioritized remediation recommendations to improve telecommunications security, prevent unauthorized access, and ensure business continuity.

SERVER CONFIGURATIONS ASSESSMENT

When conducting a Server Configurations Assessment, we will evaluate JMU's server security posture by analyzing configurations against industry-standard security benchmarks. Our objective is to identify misconfigurations, unpatched vulnerabilities, and deviations from best practices that could expose critical systems to cyber threats.

We start by identifying in-scope servers, which may include:

- Windows and Linux servers
- Database servers (SQL, MySQL, PostgreSQL, etc.)
- Web servers (Apache, Nginx, IIS, etc.)
- Application servers and domain controllers

We will then conduct automated security configuration scans using Tenable Nessus, assessing the servers against:

- CIS Benchmarks for system hardening
- DISA STIGs (Department of Defense security guidelines)

Once the scans are complete, we will analyze the findings and generate a report using our internal report generation system, PlexTrac. This report will include:

- Identified misconfigurations and deviations from security best practices
- Unpatched vulnerabilities and missing security updates
- Non-compliant user access settings and privilege mismanagement
- Actionable hardening recommendations for each server type

After presenting our findings to key stakeholders, we will provide guidance on remediation strategies, including applying security patches, enforcing hardening measures, and ensuring compliance with regulatory frameworks. If needed, we will also conduct a remediation validation assessment to verify that corrective actions have been successfully implemented.

FIREWALL AND ROUTER SECURITY ASSESSMENT

Our Cybersecurity consultants will conduct a firewall review to ensure that they are configured correctly and do not have security gaps. The process of reviewing the firewall will involve looking for unrestricted or insecure ports that are allowing traffic, confirming if firewall placement is effective and correct, analyzing the current firewall rules to determine if any of them are potentially letting in dangerous traffic, and ensuring that unauthorized access to the firewalls is not possible. Steps include:

- Reviewing the network diagram for flaws
- Reviewing information flows in and out of the firewalls confirming it is configured appropriately to restrict data flow to only necessary network sources/destinations
- Reviewing the approved services, protocols, and ports on the firewall and compare to requirements
- Reviewing the firewall rule set to identify potentially overly permissive rules
- Reviewing the firewall configuration
- Scanning the configuration file with our vulnerability scanning solution to compare configuration against security benchmarks like CIS and DISA STIGs (Tenable Nessus/Nipper)

We will conduct our analysis and provide a detailed report with findings. Along with this report, we will provide configuration and rule recommendations to better optimize the security and performance of your firewalls.

The assessment on the routers will be similar, but we will focus on some common security flaws found in routers like:

- Configured accounts follow the principal of least privilege
- Weak or default administrative passwords
- Weak WiFi credentials (if applicable)
- Weak levels of encryption in use
- SSH or Telnet access is not restricted
- Vulnerable firmware installations
- Scanning the configuration file with our vulnerability scanning solution to compare configuration against security benchmarks like CIS and DISA STIGs (Tenable Nessus/Nipper)

We will conduct our analysis and provide a detailed report with findings. Along with this report, we will provide configuration and rule recommendations to better optimize the security and performance of your firewalls and routers.

DATABASE ARCHITECTURE SECURITY ASSESSMENT

During this engagement, we will conduct thorough assessments of JMU's databases to detect any potential security flaws that may be existent. Our auditors will go over the current configuration baselines and point out where potential misconfigurations or vulnerabilities may lie. With information on how the databases on the domain are currently configured, we can compare them to numerous secure baselines like DISA STIGs or CIS Benchmarks. We will analyze any policies and procedures around patching and security configurations as well and make recommendations where these areas can be improved. Ultimately, we will look at the following:

- Known vulnerabilities for current database version
- Access Control implementation for the database
- External Objects in use by the database
- How the database connects to other systems and vice versa
- Availability assessment of the database to determine coverage in case of disaster or outage
- Implemented baselines and compliance to said baselines
- Protection and monitoring tools implemented on the database server (Antivirus, Patch Management Tool, Auditing/Logging Tools, etc.)
- Current patch level and missing patches
- Continuous monitoring policy and how well it is being followed for the database servers
- Backup configuration, including schedule, backup location, and restoration plan
- Encryption of the database

Through our detailed penetration testing methodology described in a later section, we will be able to identify and discover a lot of information about the databases on the network. This includes:

- Enumeration of database OS and version (Nmap Port Scans)
- Enumeration of vulnerabilities the database may suffer from (Nessus Vulnerability Scans)
- Enumeration of out-of-date services or applications on the database server (Nessus Vulnerability Scans + Nmap Port Scans)
- Susceptibility to exploits related to discovered services running on the server
- Susceptibility to password attacks (brute force, dictionary, etc.)

With the above approach, we will be able to provide JMU with a holistic report on the security of its databases and provide remediation actions to improve the overall security

External/Internal/Active Directory Penetration testing Methodology

When conducting an internal and external penetration test for JMU, Anthony Timbers LLC will be following a specific methodology to ensure that every aspect of JMU's network is tested for any vulnerabilities. We typically follow the general ethical hacking phased approach which includes the following phases:

1. Preparation
2. Reconnaissance
3. Scanning and Enumeration
4. Gaining Access
5. Maintaining Access
6. Clearing Tracks
7. Report Writing

During the preparation phase, we will hold meetings with JMU and go over exactly what the test will cover, what your needs are, gather information about the network, gather information needed to conduct the penetration test, and compile rules of engagement document that outlines important points like target IP addresses/URLs, what we can and cannot do, and various liability points. We will not conduct any activities that could be potentially detrimental to the network or are not authorized beforehand.

The Reconnaissance phase involves leveraging Open-Source Intelligence (OSINT) tools to find any publicly available information on the domain and the target network itself. Using several tools including Google, Recon-ng, Shodan.io, and others, we can see if there is any information publicly available that would allow hackers to exploit the network or could assist in exploiting/learning about the network itself. We would search for things like compromised user credentials, publicly exposed sensitive information about the network, and any information we could possibly use to learn more about the network.

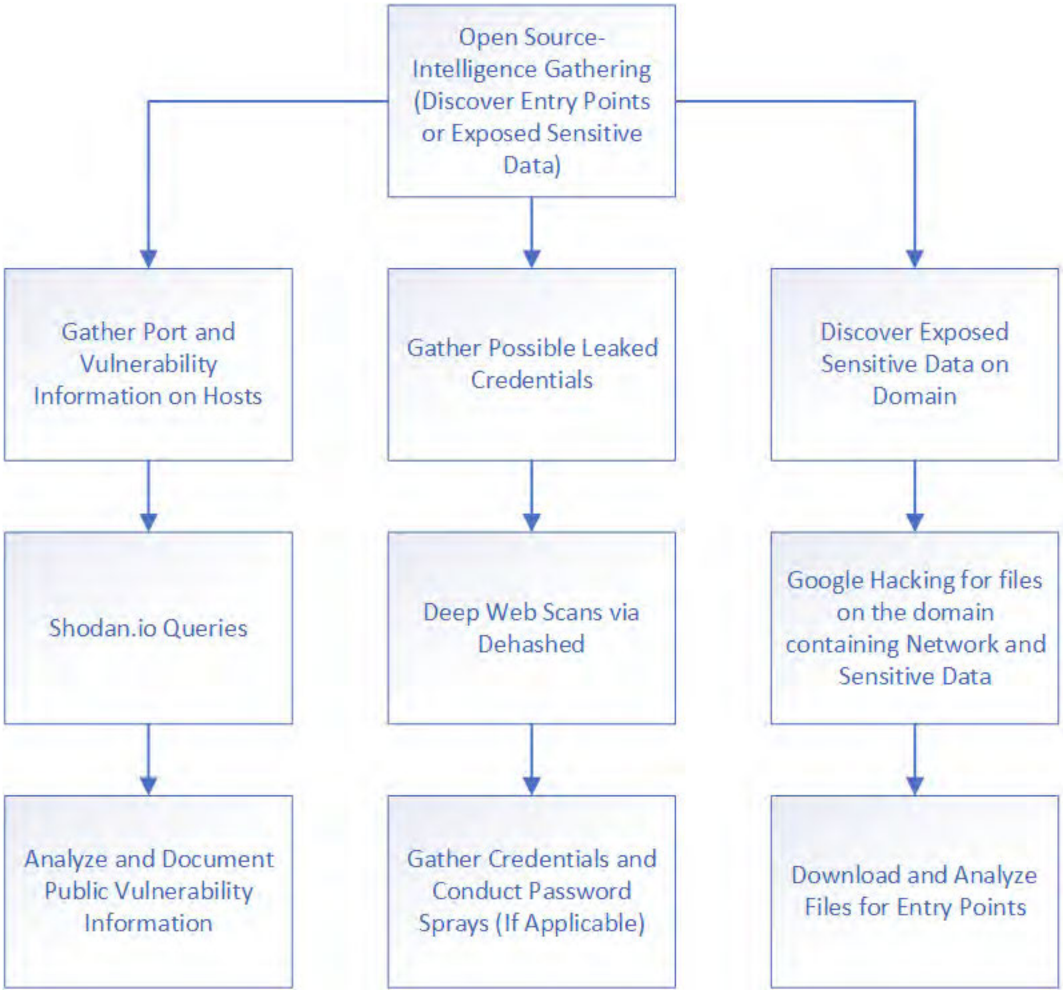

Open Source-Intelligence Gathering (Discover Entry Points or Exposed Sensitive Data)
Gather Port and Vulnerability Information on Hosts
Gather Possible Leaked Credentials
Discover Exposed Sensitive Data on Domain
Shodan.io Queries
Deep Web Scans via Dehashed
Google Hacking for files on the domain containing Network and Sensitive Data
Analyze and Document Public Vulnerability Information
Gather Credentials and Conduct Password Sprays (If Applicable)
Download and Analyze Files for Entry Points

Figure 1 - OSINT Attack Tree

Following this, we could conduct scanning and enumeration. This phase includes us actively connecting to your systems using a variety of tools like port scanners, vulnerability scanners, and others to actively discover vulnerabilities. This is typically where we will build our list of points where we can attack the network and get an idea of how we can exploit it. We will spend this time looking for vulnerable services, out-of-date systems, or exposed ports that could allow us access to the network using common hacking tools like Nmap or Nikto. For web application testing, this stage also involves both automated and manual testing of the application as well for things like SQL Injection, Cross-Site Scripting (XSS), and other OWASP top 10 vulnerabilities. We will be scanning for open vulnerabilities like outdated services running, vulnerable open ports, and other vulnerabilities discoverable with common hacking tools like Nmap. We'll scan all 65535 TCP/UDP ports (if desired) on each provided host for maximal coverage and to uncover any publicly available services. Vulnerability scans using Tenable.io will be conducted during this phase as well to find potential vulnerabilities that are visible from the outside.

The gaining access phase is simply the stage where we launch attacks and try to gain access to the systems. Based on findings in the previous phases, we will attempt to exploit the targets and determine what kind of information or access we can gain. Please note that we will only exploit targets if given prior permission by JMU. This is where we will determine if your systems are susceptible to malware and other cyber-attacks. One thing that sets us apart from others is that we always focus on manual testing followed by automated testing. To get optimal results and to truly figure out if you are susceptible to attack, manually attempting to exploit systems and vulnerabilities is vital. Instead of leaning on tools like Metasploit for the whole assessment, we use manual tools and skills primarily to penetrate systems first and then move to tools like Metasploit. We will download and modify exploits (from https://exploit-db.com for example) that we believe your systems may be vulnerable to and attempt to use them manually to confirm that they do or do not work. Automated tools are used as well secondarily to provide full coverage. This is where we will run Metasploit and see if there are any easily exploitable vulnerabilities or something that was missed during manual testing. We can import the Nmap scan results into Metasploit and let it enumerate potential vulnerabilities to exploit quickly. We also may attempt to conduct password attacks like brute force or dictionary attacks if we discover any type of login page. We typically see things like firewalls, VPNs, and mail servers exposed to the world, so we can test the login pages for them and attempt to gain access via password attacks. We will also look for common attack vectors like exploitable RDP or SMB setups.

The next phase, maintaining access, refers to how we would maintain access to any systems that we successfully exploited. The first step, however, is to escalate our privileges. We will attempt to gain administrator-level privileges if we do not already have them by doing a full enumeration on the host system. This can vary based on if the host is Windows or Linux, but this includes using the command line to learn information including:

- Operating System Version
- Current Hotfix Versions
- Currently running services and versions
- Installed applications and their paths
- Potential user accounts and groups
- Current user privileges
- Routing tables and networking information
- Scheduled tasks

Regardless of the outcome of the above tactics, we typically will try to maintain access in a stealthy way if possible. This could be installing a service that creates a callback to our system (a reverse shell) every time the computer is turned on, allowing us to always have easy access back into the system. This can be tricky due to most modern antivirus software, but we have experience creating custom malware that can easily bypass most antivirus systems by hiding a payload inside of a legitimate file, allowing it to be executed. Clearing tracks involves making it look like we were never there by taking actions such as deleting logs or turning off auditing while we are in a system. We will then attempt to move laterally and rinse and repeat the above methodology.

While on the network, we will also enumerate potential vulnerabilities in the AD environment and attempt to exploit them. On the flip side of this, we will audit the configurations of the domain to point out potential weaknesses and vulnerabilities. This includes going over current configurations for groups, users, and all group policies to discover where potential attack vectors or security issues may lie. Having configured and pen tested a number of Active Directory domains for government environments, we are very knowledgeable on how they should be configured for maximal security.

Some common AD weaknesses and misconfigurations we will enumerate include:

- LLMNR/NetBIOS Enabled
- Admin Passwords stored inside Group Policy Preferences
- Krbtgt Account password not reset
- Unsecured Network shares
- User/Service Accounts with weak passwords or too many permissions
- No password expiration policy
- Weak password complexity policy
- No lockout policy for accounts
- GPO edit permissions for non-privileged users

Some AD attacks we will attempt to launch during our assessment (gaining access phase) include:

- SMB Relay Attacks - Exploiting NTLM authentication by relaying captured credentials to another system to gain unauthorized access or escalate privileges. This attack targets improperly configured SMB signing settings or services that accept NTLM authentication without proper verification.
- Sniffing and Credential Harvesting Using Responder - Deploying Responder to intercept and respond to LLMNR, NBT-NS, and MDNS queries within the network. This technique captures sensitive information such as NTLM hashes, which can then be leveraged in further attacks like cracking the hash offline or relaying it to a vulnerable service to gain access.
- Pass-the-hash Attack – using captured hashes we will attempt to use them to authenticate across the domain and gain access to additional resources.
- DCSync Attack – upon gaining access to an account like a service account, we can attempt to impersonate a domain controller and request password hashes from other domain controllers
- Golden Ticket Exploitation – with privileged access to the domain controller (or after successfully launching a Pass-the-Hash or DCSync Attack), we will attempt to obtain the hash of the KRBTGT account (Key Distribution Service Account) and then use Mimikatz to generate a Ticket Granting Ticket that gives us access as a domain administrator.
- Dumping local hashes using Mimikatz
- Password Spraying using a custom script to gain access to accounts
- DCShadow Attack – with privileged access obtained, we will have our computer impersonate a domain controller by making changes to the AD's configuration schema.
- Domain Trust Exploitation – attempt to exploit trust configurations between multiple domains to enable lateral movement across domains.
- AD Privilege Escalation

Based on the outcomes from the assessment, we can generate a report on where weaknesses lie and how JMU can better configure their Active Directory domain for security.

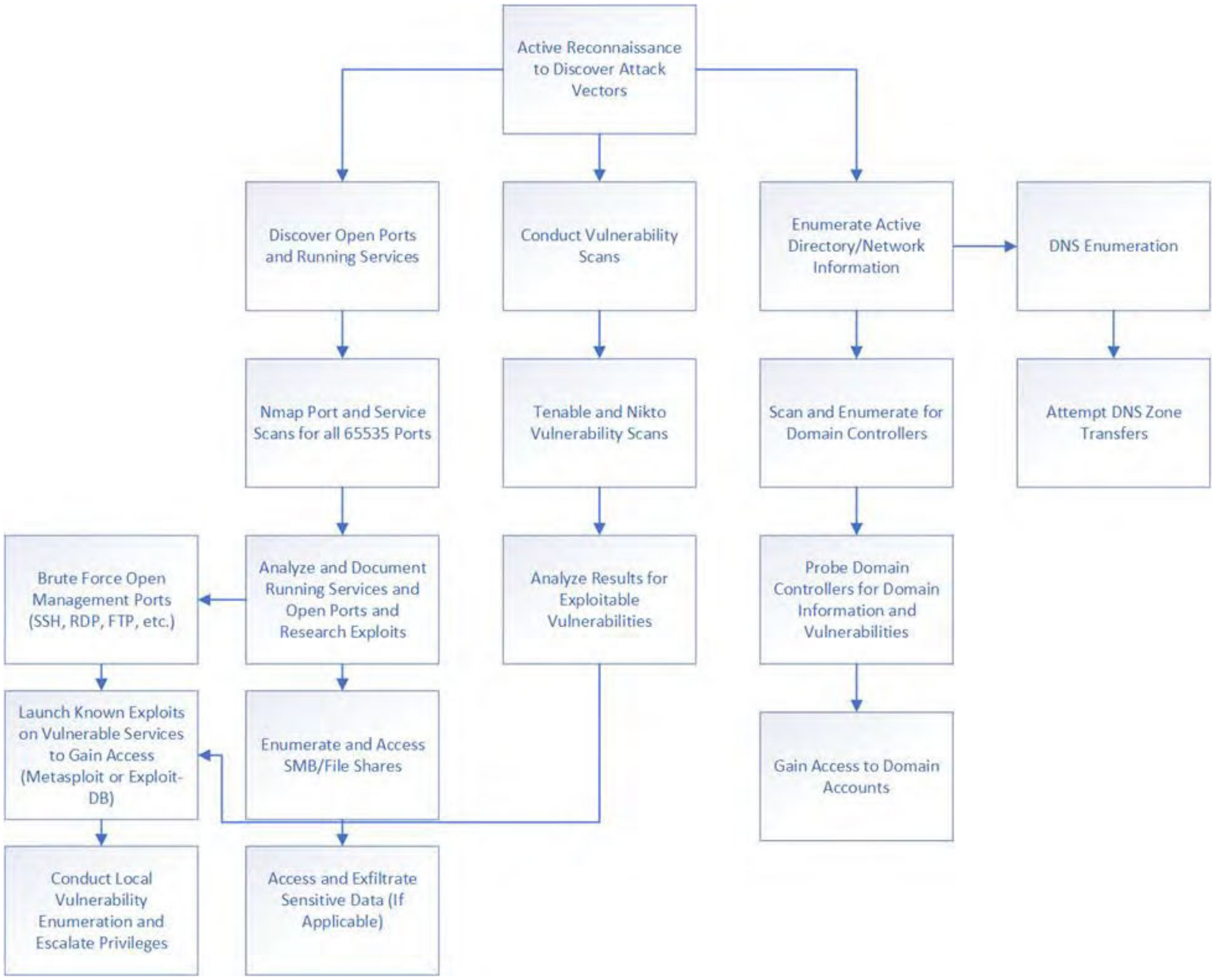

Active Reconnaissance to Discover Attack Vectors
Discover Open Ports and Running Services
Conduct Vulnerability Scans
Enumerate Active Directory/Network Information
DNS Enumeration
Nmap Port and Service Scans for all 65535 Ports
Tenable and Nikto Vulnerability Scans
Scan and Enumerate for Domain Controllers
Attempt DNS Zone Transfers
Brute Force Open Management Ports (SSH, RDP, FTP, etc.)
Analyze and Document Running Services and Open Ports and Research Exploits
Analyze Results for Exploitable Vulnerabilities
Probe Domain Controllers for Domain Information and Vulnerabilities
Launch Known Exploits on Vulnerable Services to Gain Access (Metasploit or Exploit-DB)
Enumerate and Access SMB/File Shares
Gain Access to Domain Accounts
Conduct Local Vulnerability Enumeration and Escalate Privileges
Access and Exfiltrate Sensitive Data (If Applicable)

Figure 2 - Network Penetration Test Attack Tree

At the conclusion of the penetration testing, our team will create penetration test reports that provide step-by-step details on exactly what actions they took during testing to find any potential vulnerabilities. This will allow your IT team to verify the vulnerabilities by being able to reproduce our results. The report will also contain a list of detailed remediation actions that are recommended to mitigate all discovered vulnerabilities.

WEB APPLICATION PENETRATION TESTING AND SECURITY ASSESSMENT METHODOLOGY

For any web applications that may fall in scope, the methodology that we would follow for this assessment is the Open Web Application Security Project (OWASP) Web Application Security Testing methodology. It is a very robust methodology that covers the OWASP Top 10 Web Application Vulnerabilities in detail. This methodology involves the following kinds of testing procedures:

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing

7. Input Validation Testing
8. Testing for Error Handling
9. Testing for Weak Cryptography
10. Business Logic Testing
11. Client-side Testing

The information-gathering phase relates directly to the reconnaissance and scanning/enumeration phases explained above. Configuration and deployment management testing would involve us testing the application and infrastructure for common misconfigurations that could lead to compromise. Identity management testing involves testing the user account system of the application. This involves our team testing to see if any users can perform unauthorized actions based on their roles, testing the account provisioning/user registration process, and testing for weak username policies that could lead to a compromise or information leak.

When conducting authentication and authorization testing, we would utilize a variety of techniques and tools to test for common security issues like weak password policies, broken authentication controls, weak security question answers, a vulnerable password reset process, and directory traversal vulnerabilities, and privilege escalation vulnerabilities. We would then move to session management testing to see if the application handles cookies, logins/logouts, session timeouts, and Cross-Site Request Forgery (CSRF) attempts appropriately. We test each of these, along with others, to see if they cause the application to be vulnerable in any way.

The input validation testing involves testing for those common injection vulnerabilities like XSS, SQL Injection, and others. We will be testing how the application handles input from users to see if user input is sanitized appropriately. If not, the application could be extremely vulnerable and lead to a massive compromise. We also would be testing to see if the application handles errors correctly. Testing error handling would allow us to discover if too much information about the server/application is provided when an error is thrown or if a specific error could cause any type of information leak or compromise.

Testing for weak cryptography would include us testing to see if outdated or vulnerable cryptography methods are used. This includes testing for support of SSL, TLS 1.0, TLS 1.1, and a variety of ciphers that have been confirmed as insecure and vulnerable. Support of vulnerable ciphers is a major security issue and can definitely lead to compromise if not fixed. Testing the business logic of the application would involve us testing the functionality of the application to see how it responds to being used in a way it is not intended to be used. This type of testing would allow us to discover if specific errors are thrown or information is leaked when a user uses the application in a manner that it was not intended to be used (i.e., skipping steps in a registration process to see if it causes some type of server error). Finally, client-side testing would involve us testing for many of the common client-side vulnerabilities that exist in many web applications. This means testing to see how the typical end-user is vulnerable due to security misconfigurations/vulnerabilities present in the application. The kind of vulnerabilities we would look for include HTML injection, allowing the execution of JavaScript, the presence of clickjacking, DOM-Bases XSS, and many others. While we will be primarily just scanning your web applications (confirmed from Q&A) using a web application vulnerability scanner like Burp Suite or Tenable.io, we will follow the above methodology on IP addresses/applications that appear to be potentially vulnerable and could allow us into the network.

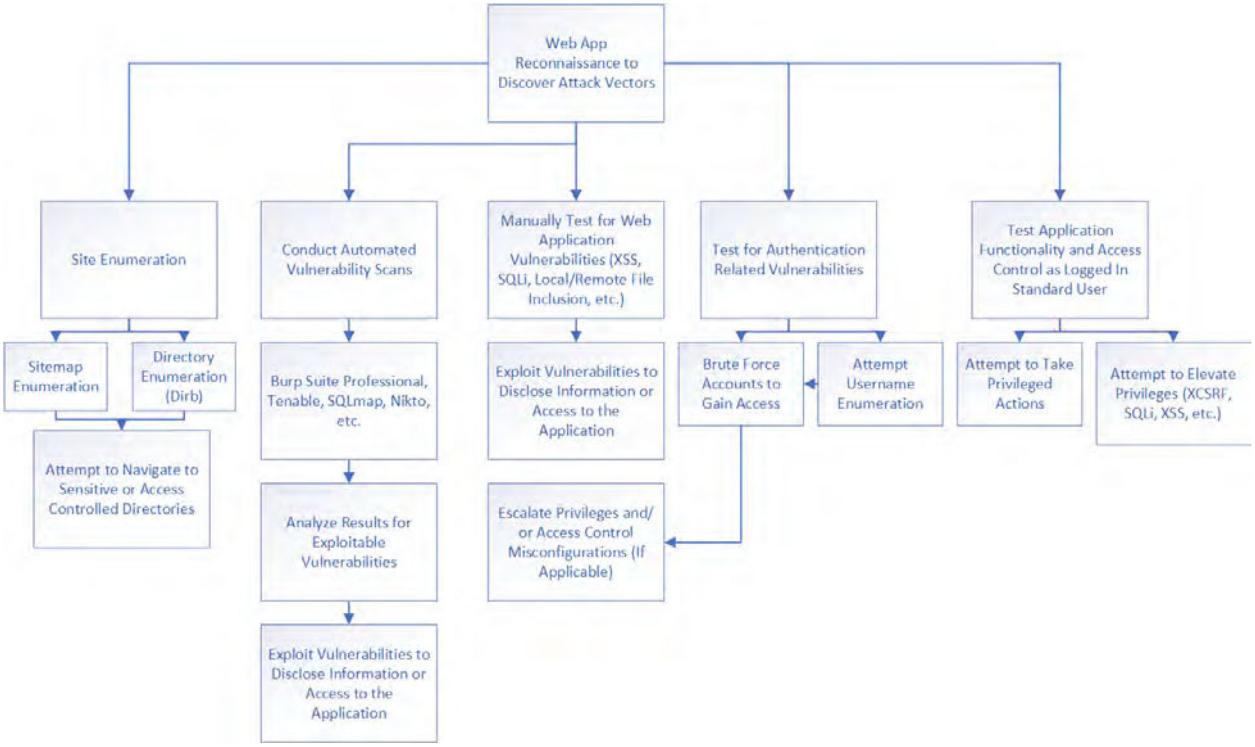

Web App Reconnaissance to Discover Attack Vectors
Site Enumeration
Conduct Automated Vulnerability Scans
Manually Test for Web Application Vulnerabilities (XSS, SQLi, Local/Remote File Inclusion, etc.)
Test for Authentication Related Vulnerabilities
Test Application Functionality and Access Control as Logged In Standard User
Sitemap Enumeration
Directory Enumeration (Dirb)
Burp Suite Professional, Tenable, SQLmap, Nikto, etc.
Exploit Vulnerabilities to Disclose Information or Access to the Application
Brute Force Accounts to Gain Access
Attempt Username Enumeration
Attempt to Take Privileged Actions
Attempt to Elevate Privileges (XCSRF, SQLi, XSS, etc.)
Attempt to Navigate to Sensitive or Access Controlled Directories
Analyze Results for Exploitable Vulnerabilities
Escalate Privileges and/or Access Control Misconfigurations (If Applicable)
Exploit Vulnerabilities to Disclose Information or Access to the Application

Figure 3 - Web Application Attack Tree

All our tests will be conducted using a variety of industry-standard penetration testing tools. Primarily, we will be utilizing Kali Linux as our penetration testing platform. Kali Linux is the most utilized operating system for conducting penetration testing assignments. It hosts a suite of hundreds of tools for penetration testing. Along with this, we will be using Burp Suite Professional. Burp Suite Professional is the number one web application penetration testing tool. With it, we can conduct accurate automatic analysis of the application and do extremely in-depth manual testing of the web application. We will be utilizing Burp Suite Professional the most during this assessment to truly discover any underlying vulnerabilities in the web application.

At the conclusion of the penetration testing, our senior consultant will create penetration test reports that provide step-by-step details on exactly what actions they took during testing to find any potential vulnerabilities. This will allow the city's IT teams to verify the vulnerabilities by being able to reproduce our results. The report will also contain a list of detailed remediation actions that are recommended to mitigate all discovered vulnerabilities.

Wireless Network Assessment

For wireless security testing, we will either send our lead auditor on-site to conduct tests on your wireless access points or remotely access systems that we send to you that are placed in the vicinity of the in-scope wireless access points. For wireless pen testing, we will be looking for potential vulnerabilities in your WiFi setup, including:

- Weak passwords or access controls to access WiFi networks or admin panels
- Weak levels of encryption in use (i.e., WPA or WEP in use)
- Out of date software that is exploitable on one of the access points
- Susceptibility to de-authentication and handshake capture attacks

Using a WiFi adapter capable of packet injection and tools like Aircrack-NG on Kali Linux, our lead consultant will attempt to find and exploit any potential vulnerabilities your wireless access points may face and report on any findings. Along with this wireless assessment, we will use our WiFi adapters to discover any potential rogue access points or evil twins that may exist on-site and report on them. We will scan the network as well in order to map out the network and determine what devices are currently connected. A report will be generated with all results from the assessment and will include an executive summary that breaks down high level results, details on steps taken and vulnerabilities discovered, and detailed remediation actions to fix any discovered issues.

Cloud Security Assessment

In order to conduct cloud security assessments, our team will use a combination of manual and automated assessments. Using Tenable, we can use a read-only account to conduct an automated scan of the environment for critical/common security misconfigurations. It will compare the current posture of the cloud environments against CIS cloud security baselines look for common cloud security issues like:

- Management ports in firewalls open to the public (3389/22)
- Access Control Misconfigurations
- Lack of MFA for administrative/root accounts
- Identity and Access Management Misconfigurations
- Other Cloud security misconfigurations

With access to cloud tenants, our consultants can also manually log in and confirm what security settings are present and missing based on their experience hardening cloud environments for various entities/organizations as well as use various automated tools to enumerate possible vulnerabilities or misconfigurations. We have extensive experience assessing and hardening cloud environments, including Azure/AWS environments for organizations that use them for applications (Multistate Partnership for Prevention, Bursys, Dock.bot, etc.) and others that use them for day-today business/productivity use (Massachusetts Office of the State Auditor, Polimaster Inc., etc.). After the assessment, our consultants will provide a report that contains details on each finding and detailed remediation actions.

Testing Location Methodology

While we are a remote organization, typically testing performed remotely, ensuring flexibility and minimal disruption to your operations. However, we understand that each client has preferences on how testing is conducted, and travel can occur if necessary. We expect to employ one of the following approaches:

1. **Remote Access via On-Site Laptops (Preferred)**:
   - We send pre-configured laptops to your site, which are then plugged into your network. Our team remotely accesses these laptops to perform penetration testing. This method is preferred as it allows us to simulate an attacker within your internal network, ensuring comprehensive and efficient testing.
2. **On-Site Testing (if required)**:
   - We send our consultants on-site to conduct penetration testing activities by connecting our laptops directly to the network.

While our processes are designed to fully facilitate remote testing, our team is available for on-site visits to ensure thorough and tailored assessments based on your unique requirements.

Tools to Be Utilized for Penetration Testing

For the penetration test, we propose utilizing a combination of industry-leading commercial tools and specialized open-source tools to ensure a comprehensive assessment. Our toolset includes:

1. **Kali Linux**: A robust and versatile platform specifically designed for penetration testing and security auditing. Kali Linux hosts a wide array of tools to address various aspects of the audit process. Some tools that are a part of the OS that could be used are as follows:

- **Nmap**: A powerful network scanning tool that discovers hosts and services on a computer network, creating a "map" of the network. Nmap is essential for identifying open ports, running services, and potential vulnerabilities.
- **Metasploit**: A widely-used penetration testing framework that helps in identifying, exploiting, and validating vulnerabilities. Metasploit facilitates advanced testing and provides detailed information for remediation.
- **Hydra**: A parallelized login cracker which supports numerous protocols to test for weak passwords.
- **Dirb**: A web content scanner capable of brute-forcing directories and files on web servers.
- **Nikto**: A web server scanner that detects potential vulnerabilities and outdated versions.
- **DNSRecon**: A DNS enumeration tool used to discover and validate various DNS records.
- **Aircrack-ng**: A comprehensive suite for assessing the security of wireless networks.

2. **Burp Suite Professional**: A powerful and widely respected tool for web application security testing. It enables detailed analysis and detection of vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application threats.
3. **Tenable Nessus Professional**: An advanced vulnerability scanning tool that provides thorough assessments of networks, identifying vulnerabilities, misconfigurations, and compliance issues. Nessus Professional delivers detailed reporting and insights to prioritize and remediate vulnerabilities effectively.

By leveraging these tools, we can conduct a thorough and meticulous audit, covering a wide range of potential vulnerabilities and ensuring that your security posture is robust and resilient against various threats.

SECURE COLLABORATION SOLUTION

To provide a secure method for collaborating and collection of evidence/sensitive information, our approach leverages our hardened and secured Government Community Cloud (GCC) tenant, which is compliant with NIST 800-171 controls.

We will utilize a SharePoint Online site specifically for this project within our GCC tenant to facilitate the collection of evidence, documentation, and delivery of reports. Our SharePoint solution will also serve as a secure, online document vault for storing and delivering documents during this engagement. This vault will be protected by advanced security measures, including encryption, MFA, access controls, and activity monitoring, to safeguard sensitive information and ensure that only authorized users can access the stored documents. This enables the organization to maintain a secure repository of compliance and supporting documentation that is both easily accessible and protected against unauthorized access.

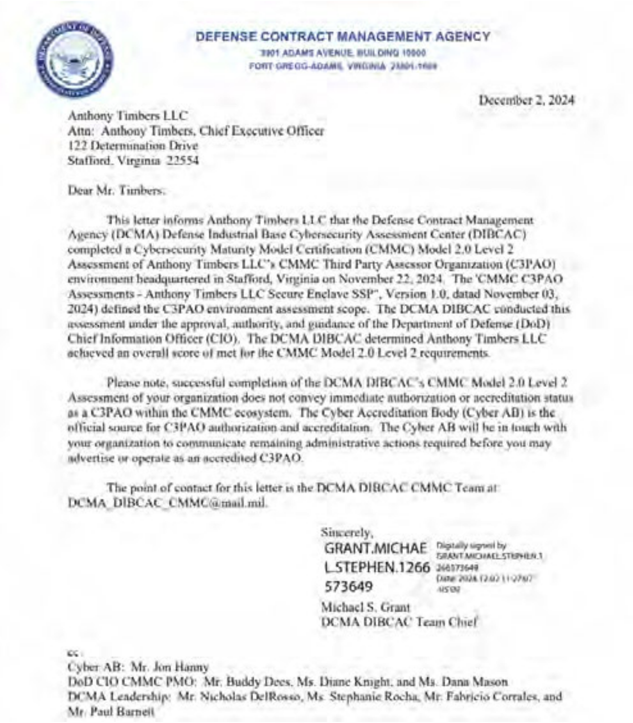
ANTHONY TIMBERS LLC DATA SECURITY

We maintain a robust cybersecurity program that covers compliance for numerous standards, including:

- NIST 800-171/CMMC Level 2
- PCI-DSS
- HIPAA
- NIST CSF
- ISO 27001

As a result, JMU can rest assured that any data that is stored by our organization is tightly access controlled and protected with the highest levels of security. Our organization practices what we preach, which is something that will separate us from other vendors. Some key features of our security program are as follows:

1. Hardened, Separate email/file sharing enclave in Microsoft 365 GCC Assessed and confirmed to meet NIST 800-171/CMMC Level 2 Requirements by DIBCAC (see below)
2. Fully managed and hardened endpoints (Antivirus, Vulnerability Scanning, Zero Trust VPN, Device Health/Posture Monitoring, SIEM Monitoring, etc.)
3. Ongoing daily and encrypted backups of critical business data
4. Ongoing vulnerability management plan that includes all endpoints and environments
5. Robust, defined Incident Response plan
6. Annual security risk assessments on the organization as a whole



DEFENSE CONTRACT MANAGEMENT AGENCY
3901 ADAMS AVENUE, BUILDING 10500
FORT GREGG-ADAMS, VIRGINIA 23801-1809

December 2, 2024

Anthony Timbers LLC
Attn: Anthony Timbers, Chief Executive Officer
122 Determination Drive
Stafford, Virginia 22554

Dear Mr. Timbers:

This letter informs Anthony Timbers LLC that the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) completed a Cybersecurity Maturity Model Certification (CMMC) Model 2.0 Level 2 Assessment of Anthony Timbers LLC's CMMC Third Party Assessor Organization (C3PAO) environment headquartered in Stafford, Virginia on November 22, 2024. The 'CMMC C3PAO Assessments - Anthony Timbers LLC Secure Enclave SSP", Version 1.0, datad November 03, 2024) defined the C3PAO environment assessment scope. The DCMA DIBCAC conducted this assessment under the approval, authority, and guidance of the Department of Defense (DoD) Chief Information Officer (CIO). The DCMA DIBCAC determined Anthony Timbers LLC achieved an overall score of met for the CMMC Model 2.0 Level 2 requirements.

Please note, successful completion of the DCMA DIBCAC's CMMC Model 2.0 Level 2 Assessment of your organization does not convey immediate authorization or accreditation status as a C3PAO within the CMMC ecosystem. The Cyber Accreditation Body (Cyber AB) is the official source for C3PAO authorization and accreditation. The Cyber AB will be in touch with your organization to communicate remaining administrative actions required before you may advertise or operate as an accredited C3PAO.

The point of contact for this letter is the DCMA DIBCAC CMMC Team at: DCMA_DIBCAC_CMMC@mail.mil.

Sincerely,
GRANT.MICHAEL.STEPHEN.1266573649
Digitally signed by GRANT.MICHAEL.STEPHEN.1266573649
Date: 2024.12.02 11:27:07 -05'00'
Michael S. Grant
DCMA DIBCAC Team Chief

cc:
Cyber AB: Mr. Jon Hanny
DoD CIO CMMC PMO: Mr. Buddy Dees, Ms. Diane Knight, and Ms. Dana Mason
DCMA Leadership: Mr. Nicholas DelRosso, Ms. Stephanie Rocha, Mr. Fabricio Corrales, and Mr. Paul Barnett

James Madison University
IT Security Auditing Services
RFP# FDC-1220

Due Date: January 30th, 2025

JMU
JAMES MADISON
UNIVERSITY

ANTHONY TIMBERS
PROTECT YOUR COMPANY WITH A CYBERSECURITY PLAN

Submitted by:
Anthony Timbers LLC
1320 Central Park Blvd Suite 200
Fredericksburg, VA 22401

Point of Contact:
Anthony Timbers
(202) 731-9376
a.timbers@anthonytimbers.com

Submitted to:
James Madison University
Procurement

TABLE OF CONTENTS

Hourly Rates 2

HOURLY RATES

Below you will find our pricing schedule, broken out by position and on vs. off site.

Position	Off-Site Hourly Rate	On-Site Hourly Rate
Project Manager	$142.98	$162.98
Quality Assurance Manager	$110.98	$130.98
Cybersecurity Manager	$152.46	$172.46
Cybersecurity Consultant I	$100.94	$120.94
Cybersecurity Consultant II	$131.04	$151.04
Cybersecurity Engineer I	$100.94	$120.94
Cybersecurity Engineer II	$131.04	$151.04
Security Analyst I	$80.88	$100.88
Security Analyst II	$95.92	$115.92
Security Analyst III	$110.98	$130.98
SOC Engineer I	$105.95	$125.95
SOC Engineer II	$121.01	$141.01
Penetration Tester I	$100.94	$120.94
Penetration Tester II	$131.04	$151.04
Application Security Analyst	$110.98	$130.98
Principal Cybersecurity Architect	$180.00	$200.00
Principal Cybersecurity Consultant	$180.00	$200.00
Principal Cybersecurity Engineer	$180.00	$200.00
PCI-DSS Qualified Security Assessor	$200.00	$220.00

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 5 Months 0

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 #

Maricopa County, AZ, 2 Years, 301 S. 4th Avenue Phoenix, AZ 85345, Aaron Moore,
Deputy Chief Information Security Officer Email – aaron.moore@maricopa.gov
Phone - 602-372-3865

City of Bakersfield, AZ, 5 Months, 1600 Truxtun Avenue Bakersfield, CA 93301, Christopher Dorroh, Security Systems Supervisor
Email – cdorroh@bakersfieldcity.us Phone - 661-326-3169

City of St. Charles 2 E. Main Street, St. Charles, IL 60174-1984 Larry Gunderson, Direction of IT Email – lgunderson@stcharlesil.gov
Phone – 630-377-4479, 2.5 Years

City of Palm Beach Gardens, 3 Months, 10500 N. Military Trail, Palm Beach Gardens, Florida, 33410 Eric Holdt, Information Technology Administrator/Director Email – EHoldt@pbgfl.com
Phone – 561-799-4142, 22

California Department of Parks and Recreation, 2 Years 715 P St, Sacramento, CA 95814 Eric Allison, IT Project Manager Email - eric.allison@parks.ca.gov
Phone - 916-306-2524

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

   Anthony Timbers LLC
   1320 Central Park Blvd Suite 200
   Fredericksburg, VA 22401

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:

ATTACHMENT B

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

Offeror Name: Anthony Timbers LLC **Preparer Name:** Anthony Timbers

Date: 01/28/2025

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: 814873 Certification date: July 2020

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 X No_____
If yes, certification number: 814873 Certification date: July 2020

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No x
If yes, certification number: ____________ Certification date: ______________

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: IT Security Auditing Services RFP# FDC-1220

Date Form Completed: 1/28/2025

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

Offeror / Proposer:
Anthony Timbers LLC
Firm

1320 Central Park Blvd Suite 200 Fredericksburg, VA 22401
Address

Anthony Timbers, 804-596-0596
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)
NA					

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

RETURN OF THIS PAGE IS REQUIRED

JMU

JAMES MADISON
UNIVERSITY

Request for Proposal

RFP# FDC-1220

Information Technology Security Auditing Services

December 17, 2024

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

VIRGINIA ASSOCIATION
OF STATE COLLEGE &
UNIVERSITY PURCHASING
PROFESSIONALS

VASCUPP

ANSWER/INQUIRY SUBMISSION FORM

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

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

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

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

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

Date: ________________

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

The following question concerns: (indicate)

RFP Document: Section (number) ________, Page ________, Paragraph _______,

____

____

____

____

____

____

____

____

____

____

____

____

Question submitted by:

____

Name Organization E-mail Address

REQUEST FOR PROPOSAL

RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

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

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

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

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

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

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

Name and Address of Firm:

____

____

____

By: ______________________________
(Signature)

Name: ______________________________
(Please Print)

Date: ______________________________

Title: ______________________________

Web Address: ______________________________

Phone: ______________________________

Email: ______________________________

Fax #: ______________________________

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

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

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

REQUEST FOR PROPOSAL

RFP # FDC-1220

TABLE OF CONTENTS

I. PURPOSE .... Page 1

II. BACKGROUND .... Page 1

III. SMALL, WOMAN-OWNED, AND MINORITY PARTICIPATION .... Page 1

IV. STATEMENT OF NEEDS .... Pages 1-3

V. PROPOSAL PREPARATION AND SUBMISSION .... Pages 3-6

VI. EVALUATION AND AWARD CRITERIA .... Page 6

VII. GENERAL TERMS AND CONDITIONS .... Pages 6-12

VIII. SPECIAL TERMS AND CONDITIONS .... Pages 12-16

IX. METHOD OF PAYMENT .... Page 16

X. PRICING SCHEDULE .... Page 17

XI. ATTACHMENTS .... Page 17

A. Offeror Data Sheet

B. SWaM Utilization Plan

C. Sample of Standard Contract

D. Zone Map

I. PURPOSE

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

II. BACKGROUND

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

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

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

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

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

IV. STATEMENT OF NEEDS

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

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

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

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

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

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

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

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

D. Billing Rate:

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

E. Additional Information

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

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

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

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

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

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

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

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

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

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

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

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

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

   a. **ELECTRONIC SUBMISSION**:

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

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

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

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

b. **PAPER SUBMISSIONS:**

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

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

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

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

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

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

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

4. Proposal Preparation

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

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

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

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

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

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

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

B. SPECIFIC PROPOSAL INSTRUCTIONS

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

1. Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required. (Electronic signature shall be accepted, i.e. Adobe Sign, DocuSign, etc.)

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

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

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

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

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

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

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

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

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

VII. GENERAL TERMS AND CONDITIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

H. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS RFPs: Failure to submit a proposal on the official state form provided for that purpose may be a cause for rejection of the proposal. Modification of or additions to the General Terms and Conditions of the solicitation may be cause for rejection of the proposal; however, the Commonwealth reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal.

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

J. PAYMENT:

1. To Prime Contractor:

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

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

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

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

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

2. To Subcontractors:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

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

2. Employer's Liability: $100,000

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

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

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

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

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

T. NONDISCRIMINATION OF CONTRACTORS: An offeror, or contractor shall not be discriminated against in the solicitation or award of this contract because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, faith-based organizational status, any other basis prohibited by state law relating to discrimination in employment or because the offeror employs ex-offenders unless the state agency, department or institution has made a written determination that employing ex-offenders on the specific contract is not in its best interest. If the award of this contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VIII. SPECIAL TERMS AND CONDITIONS

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

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

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

From: ____

Name of Offeror   Due Date   Time

____

Street or Box No.   RFP #

____

City, State, Zip Code   RFP Title

Name of Purchasing Officer: ______________________________

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

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

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

E. UNDERSTANDING OF REQUIREMENTS: It is the responsibility of each offeror to inquire about and clarify any requirements of this solicitation that is not understood. The University will not be bound by oral explanations as to the meaning of specifications or language contained in this solicitation. Therefore, all inquiries deemed to be substantive in nature must be in writing and submitted to the responsible buyer in the Procurement Services Office. Offerors must ensure that written inquiries reach the buyer at least five (5) days prior to the time set for receipt of offerors proposals. A copy of all queries and the respective response will be provided in the form of an addendum to all offerors who have indicated an interest in responding to this solicitation. Your signature on your Offer certifies that you fully understand all facets of this solicitation. These questions may be sent via email directly to the Procurement Officer listed on the signature page of this solicitation or by Fax to 540/568-7935.

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

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

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

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

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

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

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

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

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

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

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

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

3. Each prime contractor who wins an award valued over $200,000 shall deliver to the contracting agency or institution with every request for payment, information on use of subcontractors that are not Department of Small Business and Supplier Diversity (SBSD)-certified small businesses. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, FEIN number, total dollar amount subcontracted, and type of product or service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu** .

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

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

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

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

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

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

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

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

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

IX. METHOD OF PAYMENT

The contractor will be paid based on invoices submitted in accordance with the solicitation and any negotiations. James Madison University recognizes the importance of expediting the payment process for our vendors and suppliers; we request that our vendors and suppliers enroll in our bank's Comprehensive Payable options: either the Virtual Payables Virtual Card or the PayMode-X electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the Virtual Payables process will receive the benefit of being paid Net 15. Additional information is available online at:
http://www.jmu.edu/financeoffice/accounting-operations-disbursements/cash-investments/vendor-payment-methods.shtml

X. PRICING SCHEDULE

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

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

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

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

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

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

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

   Years_______ Months_________

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

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

   ____

   ____

   ____

   ____

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

   ____

   ____

   ____

ATTACHMENT B

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

Offeror Name: ___________________________________ Preparer Name: __________________

Date: ________

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

If yes, certification number: ____________ Certification date:______________

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

If yes, certification number: ____________ Certification date:______________

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

If yes, certification number: ____________ Certification date:______________

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

If yes, certification number: ____________ Certification date: ______________

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: ______________________________________ Date Form Completed:_______________

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

Offeror / Proposer:

___________________________________ ____ ___________________________________
Firm Address Contact Person/No.

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

JMU
JAMES MADISON
UNIVERSITY.

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

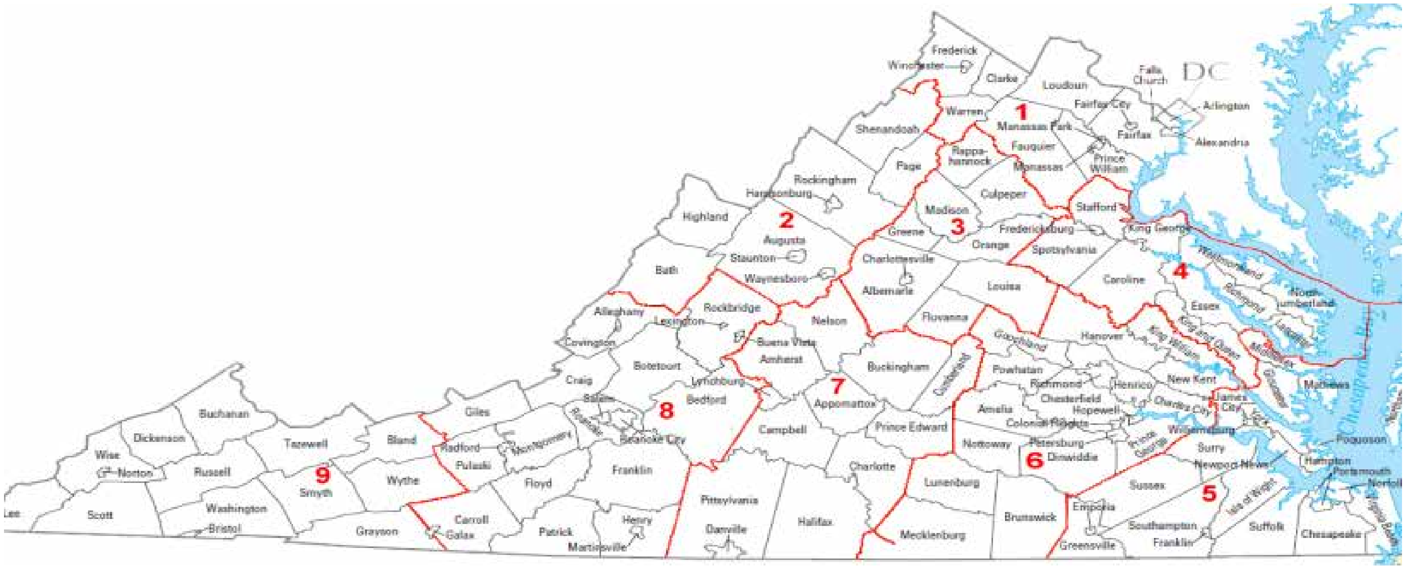
(3) The Contractor's Proposal dated ____________________and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations summary dated ____________.

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)	**Christopher Newport University (Newport News)** **College of William and Mary (Williamsburg)** **Norfolk State University (Norfolk)** **Old Dominion University (Norfolk)**	**Virginia Commonwealth University (Richmond)** **Virginia State University (Petersburg)**
Zone 7	**Zone 8**	**Zone 9**
Longwood University (Farmville)	**Virginia Military Institute (Lexington)** **Virginia Tech (Blacksburg)** **Radford University (Radford)**	**University of Virginia - Wise (Wise)**

January 10, 2025

ADDENDUM NO.: One

TO ALL OFFERORS

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

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

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

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

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

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

JMU
JAMES MADISON UNIVERSITY

January 16, 2025

ADDENDUM NO.: Two

TO ALL OFFERORS

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

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

AMS refers to JMU's Office of Audit Management Services

The following questions are answered below:

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

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

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

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

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

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

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

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

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

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

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

   Answer: Not required

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

Answer: No

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21. Are sample reports or templates available for review?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Answer: Engagements are typically more red team.

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

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

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

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

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

    Answer: Consultants are free to use any framework.

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

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

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

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

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

    Answer: Some audits may require follow-up testing.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Answer: This has not been done in the past.

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

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

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

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

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

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

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

    Answer: Allowable expenses will be discussed during planning.

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

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

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

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

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

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

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

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

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

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

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

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

67. How frequently are status reports or updates required?

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

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

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

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

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

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

    Answer: Included in flat rates.

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

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

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

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

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

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

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

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

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

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

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

    Answer: GLBA required audit is a potential engagement.

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

    Answer: Currently, JMU IT is using ISO.

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

    Answer: This contract will be made available to the VASCUPP schools for their use, should they choose to do so. This will be a cooperative contract that can be utilized by any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations

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

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

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

    Answer: At least one of the certifications.

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

    Answer:

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

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

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

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

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

    Answer: Yes

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

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

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

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

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

Answer: The current providers can be found here.

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

    Answer: See the answer to question 86 above.

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

    Answer: Yes.

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

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

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

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

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

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

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

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

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

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

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

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

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

    Answer: The university refrains from answering this question.

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

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

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

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

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

    Answer: Yes

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

Answer: Will be discussed during planning for each engagement.

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

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

101. Does the University use baseline images for systems?

Answer: Yes

102. Is formalized change management in place?

Answer: Yes

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

Answer: Will be discussed during planning if necessary.

104. How many wireless locations are in-scope?

Answer: Will be discussed during planning if necessary.

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

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

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

Answer: Will be discussed during planning if necessary.

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

Answer: Will be discussed during planning if necessary.

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

Answer: Will be discussed during planning if necessary.

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

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

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

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

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

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

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

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

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

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

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

Answer: Some academic units manage their own systems.

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

Answer: They are included in audits managed by AMS

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

Answer: AMS is JMU's internal audit department.

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

Answer: Central IT manages most IT assets.

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

Answer: Yes

119. Who tracks JMU's IT Assets?

Answer: Central IT manages most IT assets.

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

Answer: Yes

121. Who performs routine and scheduled maintenance?

Answer: Central IT for most systems

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

Answer: The current contracts expire in April of 2025.

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

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

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

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

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

Answer: We have four vendors on contract.

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

Answer: The listed examples are performed by consultants.

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

Answer: The listed examples are performed by consultants.

128. How many web applications are being assessed?

Answer: This will be determined during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

132. Will the source code be made readily available?

Answer: No

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

135. How many total IP addresses are being tested?

Answer: This will be discussed during planning.

136. How many internal IP addresses, if applicable?

Answer: This will be discussed during planning.

137. How many external IP addresses, if applicable?

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

139. Would the University prefer SWaM agencies?

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

140. Is subcontracting mandatory for SWaM-certified agencies?

Answer: No

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

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

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

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

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

Answer: This information is not readily available.

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

Answer: Instructions are on page 17 of the RFP.

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

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

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

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

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

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

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

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

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

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

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

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

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

158. What hypervisors are being used in the environment?

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

160. How many databases are in the environment?

Answer: This will be discussed during planning.

161. What platforms are these databases hosted on?

Answer: This will be discussed during planning.

162. What applications use these databases?

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

164. How many web applications are in scope?

Answer: This will be discussed during planning.

165. Where are these web applications hosted?

Answer: This will be discussed during planning.

166. What platforms do these applications run on?

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

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

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

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

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

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

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

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

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

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

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

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

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

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

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

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

Answer: This information is not readily available.

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

Answer: This information is not readily available.

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

Answer: This information is not readily available.

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

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

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

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

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

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

191. What brand of firewall equipment are you using?

Answer: This will be discussed during planning.

192. What brand of router equipment are you using?

Answer: This will be discussed during planning.

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

Answer: This will be discussed during planning.

194. What types of services does Telecommunications entail?

Answer: This will be discussed during planning.

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

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

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

Answer: We expect consultants to use their own tools.

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

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

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

Answer: The university refrains from answering this question.

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

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

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

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

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

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

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

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

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

Answer: Will be discussed during planning for each engagement.

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

Answer: This is determined during planning.

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

Answer: This is determined during planning.

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

Answer: These audits can be completed by one person.

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

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

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

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

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

Answer: No, unless determined otherwise during planning.

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

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

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

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

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

Answer: This will be determined during planning.

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

Answer: The university refrains from answering this question.

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

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

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

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

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

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

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

Sincerely,

Doug Chester
Buyer Senior
Phone: 540-568-4272