JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. UCPJMU6504

This contract entered into this 10th day of January 2023, by CampusGuard, 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 January 10th, 2023 through January 9th, 2024 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 RFP FDC-1161, dated September 12, 2022.
- (a) The Statement of Needs;
- (b) The General Terms and Conditions;
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) Addendum No. One, dated September 30, 2022.

(3) The Contractor's Proposal dated October 10, 2022 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations Summary, dated November 28, 2022;
- (b) The Commonwealth of Virginia Agency Contract Form Addendum to Contractor's Form, which shall govern in the event of conflict.
- (c) JMU IT Services Addendum, dated December 7,2022;
- (d) CampusGuard's Annual Support Agreement Statement of Work

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

CONTRACTOR:	PURCHASING AGENCY:
By: _____ (Signature)	By: _____ (Signature)
Doug Chester (Printed Name)	Andrew Grant (Printed Name)
Title: Buyer Senior	Title: Director, National Business Development

RFP # FDC-1161, Higher Education Compliance Consulting Services
Negotiation Summary for CampusGuard, LLC

November 28, 2022

1. Parties agree that this Negotiation Summary modifies RFP# FDC-1161 and the Contractor's initial response to RFP# FDC-1161, and in the event of conflict this negotiation summary shall take precedence.

2. The rate schedule is as follows:

Cybersecurity and Compliance Assessments (NIST, HIPAA, PCI, GLBA, FERPA, etc.)	Price
1 Day – Remote	$9,900.00
2 Day – Remote	$12,900.00
3 Day – Remote	$14,900.00
4 Day – Remote	$16,900.00
5 Day -Remote	$18,900.00
1 Day - Onsite	$13,400.00
2 Day - Onsite	$17,300.00
3 Day - Onsite	$20,200.00
4 Day - Onsite	$23,000.00
5 Day - Onsite	$25,900.00
Report on Compliance Assessments	**Price**
3 Day PCI DSS Report on Compliance***	$44,950.00
4 Day PCI DSS Report on Compliance***	$49,950.00
5 Day PCI DSS Report on Compliance***	$54,950.00
***Applicable to PCI DSS ONLY. One onsite visit included in pricing for the period of days indicated.	
Annual Support Agreements	**Price**
10 Hours**	$10,000.00
20 Hours**	$12,000.00
30 Hours**	$14,400.00
40 Hours**	$16,800.00
50 Hours**	$19,200.00
60 Hours**	$21,600.00
80 Hours**	$28,800.00
100 Hours**	$33,600.00
***Includes CampusGuard Central™ portal, PCI and HIPAA policy and procedure template library, quarterly external vulnerability scans, and hours for information security and compliance support.*	
Onsite Fee	**Price**
1 Day	$3,500
2 Days	$4,400
3 Days	$5,300
4 Days	$6,100
5 Days	$7,000
10 Days	*This will be handled as two 5-day trips*
▪ Note 1: The Onsite Fee includes travel time and travel and living expenses. ▪ Note 2: The Onsite Fee is assessed per visit.	

Off-Site Consulting Hours	Price
10 Hours	$3,000.00
20 Hours	$6,000.00
40 Hours	$12,000.00
60 Hours	$17,100.00
80 Hours	$22,800.00
100 Hours	$27,500.00
200 Hours	$55,000.00
CampusGuard Central ™ PCI Portal	**Price**
Includes electronic SAQs, Policy Templates, Secure Document Storage, Multiple Roles, unlimited MIDs	*Quoted per Customer*
Vulnerability Assessments & Penetration Testing (every test will be different and quoted for size and configuration based on estimated effort)	***Price***
Vulnerability Assessment (all types) - Hourly Rate	$255.00
Penetration Testing (all types) - Hourly Rate***	$255.00
License and Appliance annual fee for internal scans	$2,995.00
Social Engineering Campaigns - Hourly	$255.00
Physical Security Reviews - Hourly***	$255.00
****All services performed remotely. Requested travel and living expenses billed separately. See item 4 of Negotiation Summary below.*	
Premier Partner Services	***Price***
Premier Partner Services	Quoted by project depending on scope

Online Training Courses	***Annual Price per Subscription***	
	VASCUPP Hosted	CampusGuard Hosted
Faculty / Staff	$6.00	$8.00
Students	$1.00	N/A

- Includes the following CampusGuard OLT Courses: Information Security Awareness, PCI DSS, GLBA, HIPAA, FERPA, FACTA/Red Flags, Phishing/Spear Phishing.
- Student pricing can only be used for educational curriculum. Student employees are considered equivalent to staff.
- Minimum purchase of 100 subscriptions per institution with supplemental increments in bundles of 50 subscriptions.
- Online training courses can be hosted by the institution on their own SCORM compatible LMS.
- CampusGuard reserves the right to audit subscription usage at each customer hosted environment every six months.
- CampusGuard hosted customers are subject to hosting fees of $2,400.00 per year per institution.

Notes:

1. CampusGuard is able to provide assessments in a remote or onsite capacity. Standard assessments are remote. Confirmation to an onsite presence will be confirmed and agreed to prior to travel arrangements being procured.
2. Assessment invoice will be issued upon completion of the remote assessment interviews or on-site services as a single invoice.
3. For the Annual Support Agreement (ASA), prices will be based on the term outlined in the Order Form signed by the customer, beginning on the 1st or 15th day of the month, closest to the Order Form execution date, and concluding after a period of 12 months.
4. A separate invoice will be generated for the ASA following the assessment interviews and prior to the start of the term.

5. Following the initial one 1-year term, the ASA annual fee will increase 5% per year after the first year.
6. Invoices for the ASA will be issued annually 45 days in advance of the renewal date.
7. Travel time for requested ASA Onsite Services will be applied as the actual round-trip travel time but will not exceed 12 hours per visit. Reasonable travel and living expenses for any requested Onsite Services will be billed separately or customer can choose to apply two hours of ASA time per day in lieu of travel and living expenses.
8. All penetration testing services will be accompanied by a Rules of Engagement (RoE) that will describe each penetration testing scope of work.
9. All penetration testing services will be performed remotely. Should onsite work be requested by customer, all travel time and reasonable travel and living expenses will be billed separately.
10. Invoices for penetration testing services will be issued upon delivery of the Penetration Test Report.
11. Penetration testing pricing may or may not include a re-test. Retest will be determined during the construction of the SOW.
12. OLT pricing includes unlimited access for enrolled staff/student up to the maximum number of subscriptions.
13. OLT will be delivered via SCORM files if hosted by customer.
14. The first five hours of content customization is delivered at $1500.00. Hours following the five hours can be completed at $300 per hour.
15. For CampusGuard hosted customers a onetime custom OLT branding can be completed at $995.00.
16. For CampusGuard hosted OLT customers a onetime single sign-on service can be completed at $2,195.00.
17. The parties both understand and acknowledge that any mutually agreed modification or addition of services or other terms must be on a written and executed Order Form. Any subsequently executed Order Form shall be subject to the terms of this contract, and any conflict between different Order Forms or an Order Form and Contract shall be controlled Contract.

3. CampusGuard, LLC agrees that if a new course is added to their training portfolio, JMU will receive that course at no additional cost.

4. JMU will have two options to procure the necessary travel time and expenses for a two-day onsite visit. The first is to pay the two-day onsite fee of $4,400.00, which includes all travel time and travel expenses. The second option is to use hours from the Annual Support Agreement to accommodate for the travel and living expenses. The hours would be applied as follows: actual travel time not to exceed 12 hours and 2 hours per day to cover living expenses. In the case of a two-day onsite visit, the total would be no more than 16 hours.

5. Contractor agrees that all exceptions taken within their initial response to RFP FDC-1161 that are not specifically addressed with this negotiation summary are null and void.

6. Any third-party documentation provided to CampusGurad by JMU and the identities of perspective vendors shall be considered confidential information under this agreement.

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

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

AGENCY NAME: James Madison University

CONTRACTOR NAME: CampusGuard LLC

DATE: December 16, 2022

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

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

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

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

1. **Requiring the Commonwealth to maintain any type of insurance either for the Commonwealth's benefit or for the contractor's benefit;**

2. **Renewing or extending the agreement beyond the initial term or automatically continuing the contract period from term to term;**

3. **Requiring or stating that the terms of the attached Contractor's form agreement shall prevail over the terms of this addendum in the event of conflict;**

4. **Requiring the Commonwealth to defend, indemnify or to hold harmless the Contractor for any act or omission;**

5. **Imposing interest charges contrary to that specified by the *Code of Virginia*, §2.2-4347 through 2.2-4354, Prompt Payment;**

6. **Requiring the application of the law of any state other than Virginia in interpreting or enforcing the contract or requiring or permitting that any dispute under the contract be resolved in the courts of any state other than Virginia;**

7. **Requiring any total or partial compensation or payment for lost profit or liquidated damages by the Commonwealth if the contract is terminated before its ordinary period;**

8. **Requiring that the contract be "accepted" or endorsed by the home office or by any other officer subsequent to execution by an official of the Commonwealth before the contract is considered in effect;**

9. **Delaying the acceptance of this contract or its effective date beyond the date of execution;**

10. **Limiting or adding to the time period within which claims can be made or actions can be brought;**

11. **Limiting the liability of the Contractor for property damage or personal injury. The parties agree that this clause does not extend the Contractor's liability beyond its own acts or those of its agents/employees;**

12. **Permitting unilateral modification of this contract by the Contractor;**

13. **Binding the Commonwealth to any arbitration or to the decision of any arbitration board, commission, panel or other entity;**

14. **Obligating the Commonwealth to pay costs of collection or attorney's fees;**

15. **Granting the Contractor a security interest in property of the Commonwealth;**

16. **Bestowing any right or incurring any obligation that is beyond the duly granted authority of the undersigned agency representative to bestow or incur on behalf of the Commonwealth.**

17. **Requiring the "confidentiality" of the agreement, in whole or part, without (i) invoking the protection of Section 2.2-4342F of the Code of Virginia in writing prior to signing the agreement (ii) identifying the data or other materials to be protected, and (iii) stating the reasons why protection is necessary.**

18. **Requiring the Commonwealth to reimburse for travel and living expenses in excess of the agency policy located at** https://www.jmu.edu/financemanual/procedures/4215mie.shtml

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

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

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

AGENCY by _____

Title Buyer Senior

Printed Name Doug Chester

CONTRACTOR by _____

Title Director, National Business Development

Printed Name Andrew Grant

James Madison University
Information Technology Services Addendum

CONTRACTOR NAME: CampusGuard LLC

PRODUCT/SOLUTION: Higher Education Compliance Consulting Services

Definitions:

- Agreement: The "Agreement" includes the contract, this addendum and any additional addenda and attachments to the contract, including the Contractor's Form.
- University: "University" or "the University" means James Madison University, its trustees, officers and employees.
- University Data: "University Data" is defined as any data that the Contractor creates, obtains, accesses, transmits, maintains, uses, processes, stores or disposes of in performance of the Agreement. It includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites.
- Personally Identifiable Information: "Personally Identifiable Information" (PII) includes but is not limited to: Any information that directly relates to an individual and is reasonably likely to enable identification of that individual or information that is defined as PII and subject to protection by James Madison University under federal or Commonwealth of Virginia law.
- Security Breach: "Security Breach" means a security-relevant event in which the security of a system or procedure involving University Data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
- Service(s): "Service" or "Services" means any goods or services acquired by the University from the Contractor.

1. **Rights and License in and to University Data:** The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use the data as provided in the Agreement solely for the purpose of performing its obligations hereunder. The Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property.

2. **Disclosure:** All goods, products, materials, documents, reports, writings, video images, photographs, or papers of any nature including software or computer images prepared or provided to the Contractor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

3. **Data Privacy:**
    a. Contractor will use University Data only for the purpose of fulfilling its duties under the Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by law.
    b. University Data will not be stored outside the United States without prior written consent from the University.
    c. Contractor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill obligations under the Agreement. The Contractor will ensure that the Contractor's employees, and subcontractors when applicable, who perform work under the Agreement have received appropriate instruction as to how to comply with the data protection provisions of the Agreement and have agreed to confidentiality obligations at least as restrictive as those contained in this Addendum.
        i. If the Contractor will have access to the records protected by the Family Educational Rights and Privacy Act (FERPA), Contractor acknowledges that for the purposes of the Agreement it will be designated as a "school official" with "legitimate educational

interests" in such records, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use such records only for the purpose of fulfilling its duties under the Agreement for University's and its End Users' benefit, and will not share such data with or disclose it to any third party except as required by law or authorized in writing by the University. Contractor acknowledges that its access to such records is limited to only those directly related to and necessary for the completion of Contractor's duties under the Agreement.

d. The Contractor shall be responsible and liable for the acts and omissions of its subcontractors, including but not limited to third-party cloud hosting providers, and shall assure compliance with the requirements of the Agreement.

4. **Data Security:**
   a. Contractor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.
   b. Contractor will store and process University Data in a secure site and will provide a SOC 2 or other security report deemed sufficient by the University from a third-party reviewer along with annual updated security reports. If the Contractor is using a third-party cloud hosting company such as AWS, Rackspace, etc., the Contractor will obtain the security audit report from its hosting company and give the results to the University. The University should not have to request the report directly from the hosting company.
   c. Contractor will use industry-standards and up-to-date security tools, technologies and practices such as network firewalls, anti-virus, vulnerability scans, system logging, intrusion detection, 24x7 system monitoring, and third-party penetration testing in providing services under the Agreement.
   d. Without limiting the foregoing, Contractor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and stored at AES 256 or stronger.

5. **Data Authenticity, Integrity and Availability:**
   a. Contractor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. Contractor shall be responsible for ensuring that University Data, per the Virginia Public Records Act, is "preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration."
   b. Contractor will ensure backups are successfully completed at the agreed interval and that restoration capability is maintained for restoration to a point-in-time and\or to the most current backup available.
   c. Contractor will maintain an uptime of 99.99% or greater as agreed to for the contracted services via the use of appropriate redundancy, continuity of operations and disaster recovery planning and implementations, excluding regularly scheduled maintenance time.

6. **Employee Background Checks and Qualifications:**
   a. Contractor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of the Agreement including but not limited to all terms relating to data and intellectual property protection.
   b. If the Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, the Contractor shall perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act: Social

Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC).

7. **Security Breach:**
   a. Response: Immediately (within one day) upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Contractor will notify the University ISO at (ISO@jmu.edu), fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Contractor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.
   b. Liability:
      i. If Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Contractor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.
      ii. If Contractor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Contractor.

8. **Requests for Data, Response to Legal Orders or Demands for Data:**
   a. Except as otherwise expressly prohibited by law, Contractor will:
      i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking University Data;
      ii. consult with the University regarding its response;
      iii. cooperate with the University's requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
      iv. Upon the University's request, provide the University with a copy of its response.
   b. Contractor will make itself and any employees, contractors, or agents assisting in the performance of its obligations under the Agreement, available to the University at no cost to the University based upon claimed violation of any laws relating to security and\or privacy of the data that arises out of the Agreement. This shall include any data preservation or eDiscovery required by the University.
   c. The University may request and obtain access to University Data and related logs at any time for any reason and at no extra cost.

9. **Data Transfer Upon Termination or Expiration:**
   a. Contractor's obligations to protect University Data shall survive termination of the Agreement until all University Data has been returned or securely destroyed, meaning taking actions that render data written on media unrecoverable by both ordinary and extraordinary means.

b. Upon termination or expiration of the Agreement, Contractor will ensure that all University Data are securely transferred, returned or destroyed as directed by the University in its sole discretion within 60 days of termination of the Agreement. Transfer/migration to the University or a third party designated by the University shall occur without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities, methods, and data formats that are accessible and compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

c. In the event that the University requests destruction of its data, Contractor agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which Contractor might have transferred University data. Contractor agrees to provide documentation of data destruction to the University.

d. Contractor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Contractor's facilities to remove and destroy University-owned assets and data. Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. The Contractor will also provide, as applicable, a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Contractor will work closely with its successor to ensure a successful transition to the new service, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

10. **Audits:**

a. The University reserves the right in its sole discretion to perform audits of the Contractor to ensure compliance with the terms of the Agreement. Contractor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which Contractor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If Contractor must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, Contractor will at its expense conduct or have conducted at least annually a(n):

   i. American Institute of CPAs Service Organization Controls 2 (SOC 2) audit, or other independent security audit with audit objectives deemed sufficient by the University, which attests to Contractor's security policies, procedures, and controls. Contractor shall also submit such documentation for any third-party cloud hosting provider(s) they may use (e.g. AWS, Rackspace, Azure, etc.) and for all subservice providers or business partners relevant to the Agreement. Contractor shall also provide James Madison University with a designated point of contact for the SOC reports and risks related to the contract. This person shall address issues raised in the SOC reports of the Contractor and its relevant providers and partners, and respond to any follow up questions posed by the University in relation to technology systems, infrastructure, or information security concerns related to the contract.

   ii. vulnerability scan of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement; and

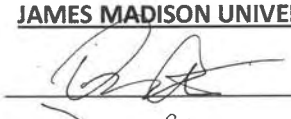
   iii. formal penetration test performed by qualified personnel of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement.

c. Additionally, Contractor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under the Agreement. The University may require, at University expense, the Contractor to perform additional audits and tests, the results of which will be provided promptly to the University.

11. **Compliance:**
    a. Contractor will comply with all applicable laws and industry standards in performing services under the Agreement. Any Contractor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Contractor upon request.
    b. To the extent applicable to the design and intended use of the service, Contractor warrants that the service it will provide to the University is fully compliant with and will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or Contractor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

12. **No End User Agreements:** Any agreements or understandings, whether electronic, click through, verbal or in writing, between Contractor and University employees or other end users under the Agreement that conflict with the terms of the Agreement, including but not limited to this Addendum, shall not be valid or binding on the University or any such end users.

IN WITNESS WHEREOF, the parties have caused this addendum to be duly executed, intending thereby to be legally bound. In the event of conflict or inconsistency between terms of the Agreement and this Addendum, the terms of this Addendum shall prevail.

	JAMES MADISON UNIVERSITY		**CONTRACTOR**
SIGNATURE:		SIGNATURE:	
PRINTED NAME:	Doug Chester	PRINTED NAME:	Andrew Grant
TITLE:	Buyer Senior	TITLE:	Director, National Business Development
DATE:	1/10/23	DATE:	December 7, 2022

CYBERSECURITY AND COMPLIANCE

Annual Support Agreement

ANNUAL SUPPORT AGREEMENT (ASA)
STATEMENT OF WORK

CampusGuard LLC ("CampusGuard") will deliver the services described below for James Madison University ("Customer").

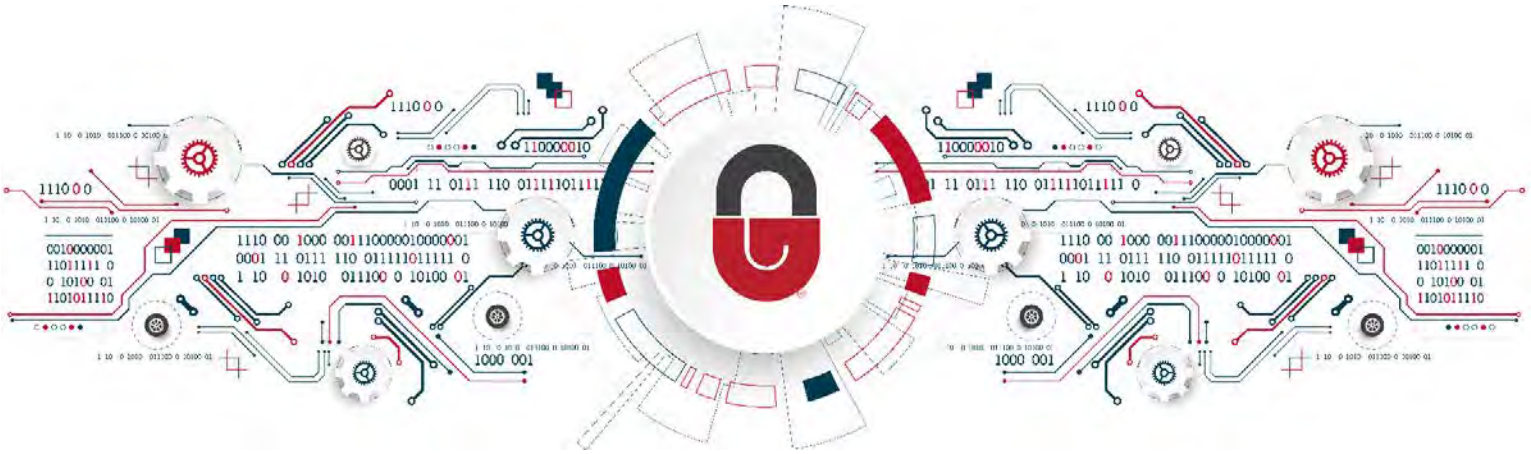
Annual Support

The CampusGuard Annual Support program includes the following:

1) Access to the CampusGuard Central® Portal
2) Access to the full library of CampusGuard policy and procedure templates
3) Quarterly External Vulnerability Scans as required for PCI compliance
4) The following services are available up to the Max # of Hours per Year
   a. Cybersecurity and Compliance Advising, Remote Support, Telephone/Email Support from your CampusGuard Team
   b. Information security and compliance policy review and/or development assistance
   c. Review and feedback on new technologies
   d. Evaluate current third-party relationships
   e. Review and feedback on new third-party relationships
   f. PCI SAQ assistance from certified PCIP and QSA professional team
   g. On-demand, Quarterly or Annual Penetration Testing, including External and Internal(1) Network, Wireless, Mobile and Application Pen Testing
   h. On-demand, Quarterly or Annual External and Internal(1) Vulnerability Scanning
   i. Cybersecurity and Incident Response Planning (IRP) Tabletop Exercises
   j. Social Engineering including Phishing/Spear Phishing Campaigns
   k. Red Teaming Exercises
   l. Password Auditing
   m. One Annual Account Review by your CampusGuard team
   n. Travel time for requested Onsite Services will be applied as the actual round trip travel time, but will not exceed twelve (12) hours per visit(2)

(1) Quarterly or Annual Internal Penetration Testing and Vulnerability Scanning services will require the purchase of a device and software license for $3,295/yr. if a device is required. One-time internal scan and penetration services will incur a one-time $200 device shipping & handling fee if a device is required.

(2) Reasonable travel and living expenses for any requested Onsite Services will be billed separately or customer can choose to apply two (2) hours of ASA time per day in lieu of travel and living expenses.



REVISED

CampusGuard Response to RFP# FDC-1161

Higher Education Compliance Consulting Services

Prepared for:

Doug Chester, Buyer Senior,
Procurement Services
Procurement Services MSC 5720
540.568.4272
chestefd@jmu.edu

Prepared by:

Andrew Grant, Director of National Business Development
CampusGuard
419.873.7016
agrant@campusguard.com

Table of Contents

REQUEST FOR PROPOSAL
RFP# FDC-1161

Issue Date: **September 12, 2022**

Title: **Higher Education Compliance Consulting Services**

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

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

Sealed Proposals Will Be Received Until 2:00 PM on October 12, 2022 for Furnishing The Services Described Herein.

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

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

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

Name and Address of Firm:

CampusGuard LLC

4740 N Cumberland Ave, Suite 365

Chicago, IL 60656

By: _____
(Signature in Ink)

Name: Andrew Grant
(Please Print)

Date: 10/10/22

Title: Dir, Nat'l Business Development

Web Address: www.campusguard.com

Phone: 419.873.7016

Email: agrant@campusguard.com

Fax #: 847.696.0564

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

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

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

Plan and Methodology

RFP Section V.B.2 and Section IV.A.1

PCI DSS Consulting Services

a. Describe the firm's experience with the Payment Card Industry Data Security Standards and the administration of those standards within the higher education community.

CampusGuard has been a certified QSA and ASV Company providing PCI consulting services since our inception in 2009.

CampusGuard is certified by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) organization providing services in North America and Australia. Of approximately 390 QSA companies and 85 ASV firms certified by the PCI SSC, CampusGuard is the only company with the sole focus of providing PCI compliance products and services to campus-based communities such as higher education. We have unparalleled experience and focus on providing the very highest levels of PCI compliance services.

CampusGuard has performed over a thousand PCI assessments for our customers. Having this experience has allowed us to develop a knowledge base of solutions for every type of payment environment. CampusGuard will bring this wealth of knowledge to the University and other institutions of higher education. When CampusGuard reports on elements and security controls in the existing environment that are not in line with the PCI DSS, your CampusGuard team will work with you to find feasible, economical, and practical recommendations and remediation plans to correct all non-compliant areas.

We specialize in performing PCI assessments, Report on Compliance (ROC) services, ASV and vulnerability scans, and penetration and segmentation testing. We have also developed a PCI Management Portal which includes an entire PCI policy and procedure template library and created our own PCI online training modules —and can apply these skills and products effectively for the campus environment because we know it is markedly different from more traditional PCI environments.

b. Describe the methodology used to maintain PCI compliance at a university.

CampusGuard has developed an approach and methodology that takes into consideration information security best practices while focusing the review on the PCI DSS and applying those standards in a diverse higher education environment. University business processes, and the networks that support them, are analyzed for adherence to the PCI DSS. Departments and the IT organization are provided PCI awareness training. Departments that handle or are involved with payment card data are interviewed for gaps in compliance. After this thorough review, CampusGuard delivers a detailed findings report along with a roadmap to guide each customer to full compliance. Using the Report, CampusGuard and the institution will work through gaps identified in the report to address and remediate vulnerabilities. Once, remediated, your

RFP Section V.B.2 and Section IV.A.1.b

dedicated Customer Relationship manager and subject matter expert team will provide continued consultation and services necessary to maintain that ongoing complaint status.

Phase 1: Charter Meeting

The project is initiated with a kick-off call to re-state objectives and align all participants to roles and responsibilities, communication methods, and schedules. The charter meeting serves to get all participants introduced and establishes key dates and timelines and discusses methodologies and tools. During this meeting, a detailed itinerary and agenda will be covered for the assessment.

Phase 2: Information Gathering and Preparation

CampusGuard will provide the University with the necessary tools to assist in the task of collecting required documentation and evidence for the assessment. Documentation includes, but is not limited to, security policies and procedures, configuration documents, and network diagrams. During this stage, CampusGuard will schedule periodic communication with the University to collect the necessary documentation.

CampusGuard will review and analyze all submitted documentation and evidence against that which is required for validating PCI DSS compliance. Any areas of non-compliance shall be identified, documented, and reported to the University for appropriate action in the Final Findings Report.

Phase 3: Assessment Interviews

CampusGuard conducts the interview portion of the assessment. As required by the PCI DSS, CampusGuard will provide experienced, certified QSA to perform the compliance assessment. The assessment includes interviews with key business and IT operations personnel (designated by the University) and review of applicable requirements as outlined in the PCI DSS. Specifically, the assessment interviews will include the following:

- Inventory of components of the University's payment card environment
- Review and analysis of relevant policies and procedures (both organizational and department level)
- Analysis of the environment to define the cardholder data environment (CDE)
- Identification and analysis of relevant third-party vendor relationships

Phase 4: Review Information from Assessment

Your CampusGuard team will review all information obtained during the interviews. At the end of the interviews, the Security Advisor will debrief the PCI Team on all pertinent activities and deliver a high-level, interim report to the PCI Team and executive level sponsors. This report identifies the highest priority risks the organization faces and possible remediation steps.

RFP Section V.B.2 and Section IV.A.1.b

Phase 5: Presentation of Final Findings Report

The Final Findings Report and Roadmap is typically delivered within twenty to thirty business days depending on the complexity of the findings. This report will provide information about all of our findings during the assessment phase of the project. It will include the details from the department visits, the network review meeting, and the initial scans, as well as our recommendations for any remediation that may be necessary. All findings will be cross referenced to the PCI DSS and will include the associated priority as defined by the PCI Security Standards Council. The Roadmap is a component of the Final Report that will provide a proposed detailed project plan for the University PCI Team to follow in order to achieve compliance.

- CampusGuard presents findings and recommendations to the customer team. We report on elements in the existing environment and security controls as evaluated against the specific requirements within the PCI DSS.
- We provide a detailed report indicating areas of non-compliance.
- We provide feasible, economical, and practical remediation plans to correct all non-compliant areas.
- We provide a high-level strategy for achieving PCI compliance, allowing for an appropriate prioritization of PCI-related work efforts. This will include a list of tasks and estimated time/labor requirements to become PCI DSS compliant.

Phase 6: Remediation

The University takes action to modify the CDE for PCI-based findings described in the Final Findings Report. Remediation tasks may include technological changes such as newly deployed systems or devices, system configuration changes, firewall policy changes as well as adjustments to roles, responsibilities, and internal processes. Changes may require the adjustment of existing policies and procedures, re-assessment, re-testing, etc.

Phase 7: Prioritized Approach

Approved by the PCI Security Standards Council, the Prioritized Approach assists organizations incrementally protect against the highest risk factors and escalating threats while on the road to compliance. The Approach and its milestones are intended to provide the following benefits:

- Roadmap to use to address risks in priority order
- Pragmatic approach that allows for “quick wins”
- Supports financial and operational planning
- Promotes objective and measurable progress indicators

RFP Section V.B.2 and Section IV.A.1.b

The Prioritized Approach provides a roadmap of compliance activities based on risk associated with storing, processing, and/or transmitting cardholder data. The roadmap helps to prioritize efforts to achieve compliance, establish milestones, lowers the risk of cardholder data breaches sooner in the compliance process, and helps University management objectively measure compliance activities and risk reduction by department.

The Prioritized Approach includes six milestones. The matrix below summarizes the high-level goals and intentions of each milestone.

	Milestone	Explanation
1	**Remove sensitive authentication data and limit data retention**	This milestone targets a key area of risk for entities that have been compromised. If sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If the data is not needed, delete it.
2	**Protect the perimeter, internal, and wireless networks**	This milestone targets controls for points of access to most compromises—the network or a wireless access point.
3	**Secure payment card applications**	This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your systems**	Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and CDE.
5	**Protect stored cardholder data**	For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protections mechanisms for that stored data.
6	**Finalize remaining compliance efforts, and ensure all controls are in place**	The intent of milestone six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

RFP Section V.B.2 and Section IV.A.1.b

Phase 8: Ongoing Advisory Services (after PCI Assessment)

CampusGuard provides ongoing guidance, training, vulnerability scanning, and penetration testing in partnership with the University to ensure continued compliance with the PCI DSS. We provide continuing guidance and ongoing support as a member of your overall PCI Team. The partnership with the University is enhanced as CampusGuard will always be available to assist with compliance efforts, department training, and answering PCI-related questions to address business and technical issues, as well as provide the vulnerability scanning and penetration testing required by the PCI DSS. In addition, throughout the term of the agreement, CampusGuard keeps the University up to date on the latest trends in information security, the latest news from the PCI Council, and overall information about new threats that have been identified. Through your dedicated Customer Advocate Team (QSA and PCIP), you will be surrounded by experts who have your best interest in mind.

CampusGuard provides an **Annual Support Agreement** that includes the following:

- Security Advisor/QSA assigned as a member of the University's PCI Team
- CRM/PCIP assigned as a member of the PCI Team
- Ongoing advising services/hours as defined in the Cost Proposal
- Unlimited access to the Compliance Management Portal, CampusGuard Central®
- Access to full inventory of Policy and Procedures Templates

Ongoing advisement can be used for activities such as:

- Cybersecurity and Compliance Advising, Remote Support, Telephone/Email Support from your CampusGuard Team
- Information security and compliance policy review and/or development assistance
- Review and feedback on new technologies
- Review and feedback on current or new third-party relationships
- PCI SAQ completion assistance and review
- On-demand, Quarterly or Annual Penetration Testing, including External and Internal Network, Wireless, Mobile and Application Pen Testing
- On-demand, Quarterly or Annual External and Internal Vulnerability Scanning
- Cybersecurity and Incident Response Planning (IRP) Tabletop Exercises
- Social Engineering including Phishing/Spear Phishing Campaigns
- Red Teaming Exercises
- Password Auditing

RFP Section V.B.2 and Section IV.A.1

c. Describe the firm's role in the university's security program.

CampusGuard strives to be a partner to the University in maintaining and expanding your PCI compliance program.

A major outcome of the PCI assessment is identification of areas that will not meet the control, documentation, or policy requirements of the PCI DSS. CampusGuard assists customers with the PCI remediation process and provides ongoing advising, training, vulnerability scanning, and penetration testing in partnership to assure continued compliance with the PCI DSS, including when PCI DSS version 4.0 is released (see below for more details). Specifically included services are:

- Maintain the detailed project roadmap that guides the University with key milestones and tasks toward full compliance
- Guidance and recommendations for any non-compliant areas.
- Review of compensating controls if applicable.
- Access to full library of policy and procedural templates
- Skilled, technically knowledgeable representation (dedicated CRM/QSA team) to assist in answering questions concerning your remediation plan and compliance timeline.
- Work with the institution as an extension of the PCI team to help develop processes, and action plans to address various PCI needs.
- Scheduled project management meetings to track defined tasks and ensure key milestones are being met
- Help to define third-party vendor oversight program.
- Review of current hosting providers and web applications
- CampusGuard's team can assist in the review of new vendor relationships to ensure new services or applications will not impact the overall PCI compliance status of the institution.
- CampusGuard will also provide templates for third-party service provider contract language, checklists for verifying compliance, and can participate in vendor discussions regarding necessary compliance documentation
- The CampusGuard Compliance Portal can also be used to track and monitor annual compliance documentation requirements.

A new version of the PCI DSS (PCI DSS 4.0) was released March 31, 2022. With this update, there are increased controls for verifying scope and monitoring requirements. According to the PCI SSC, the priorities for PCI DSS v4.0 include strengthening security and adding flexibility. The new standard includes:

- New requirements: New and revised requirements to address evolving risks and threats to payment data and to reinforce security as a continuous process.
- New focus on security objectives: Requirements and validation options are redesigned to focus on security objectives to support organizations using different methodologies to meet the intent of PCI DSS requirements.

RFP Section V.B.2 and Section IV.A.1.c-d

CampusGuard will assist all customers with how the new DSS affects their environment(s) and how they may address such changes should their environment be out of compliance with the new DSS. CampusGuard will also provide updated templates and guidance to policies and procedures based on applicable changes within PCI DSS version 4.0.

d. Describe the online system/interface the firm provides and how Self-Assessment Questionnaires (SAQ) are completed through the system.

CampusGuard has developed a compliance management portal, CampusGuard Central®, in direct response to the unique needs of multi-campus organizations. This means that you can easily view the progress each department is making toward PCI compliance. Documents such as network drawings, configuration documentation, and SAQs can be retained in the portal for reference and verification to your acquirer for compliance. Major features include:

- Customized access for Administrators to view multiple campuses, departments, and merchants
- Colorized dashboard with progress icons to quickly identify areas of focus
- Integrated scanning requests, tracking, and reporting
- Convenient access to library of templates and articles
- Secure document locker access for all with role-based accessibility
- Print or export reports in various formats (CSV, TXT, PDF, JSON)
- Ability to create summary SAQs based on various selection criteria
- Access the site using single sign-on (SSO)

These features enable the University to more easily manage the PCI compliance project that may have the scope of multiple campuses and/or departments that are considered in the cardholder data environment. Multi-level reports are available to track compliance by merchant ID, department, and building, affording administrators to have a grasp of the full compliance picture of the entire enterprise.

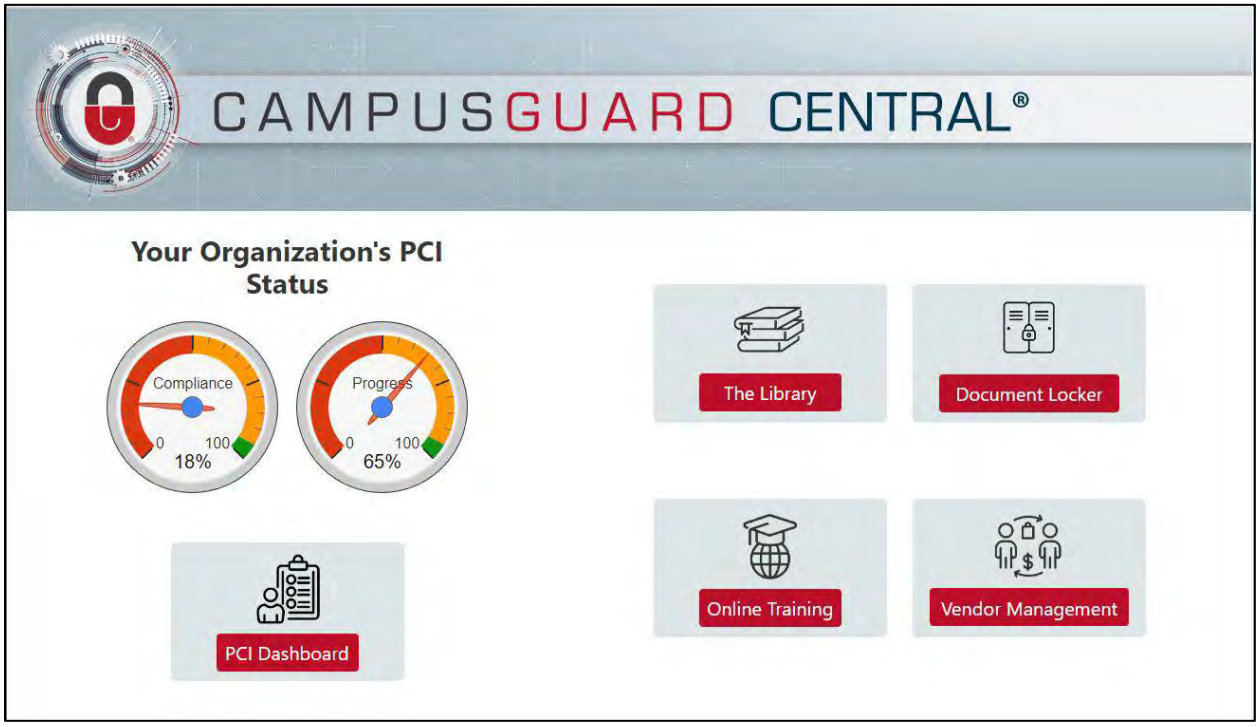
Benefits include:

- Simple user interface is easy to use, and permission-based access ensures each user only sees what they need to
- Orientation and training are provided prior to the SAQ completion process
- Staff and departments have the ability to speak to an experienced QSA or PCIP who knows the University and higher education environments
- Through the year as changes are made, individual SAQs can be updated and centrally monitored
- Ability to track progress as departments work through their individual SAQs

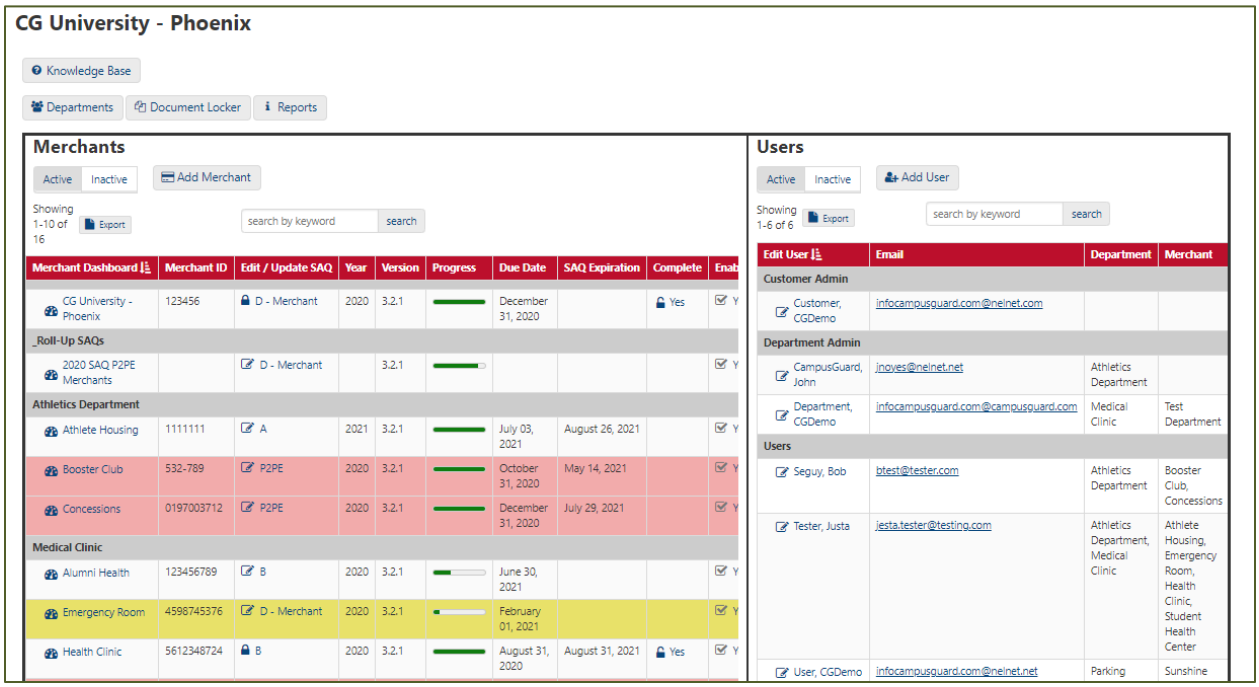
The Portal provides departments the tools needed to create and manage their SAQs. CampusGuard provides guidance and ongoing support as each department completes their SAQ.

RFP Section V.B.2 and Section IV.A.1.d

Initial Landing Page

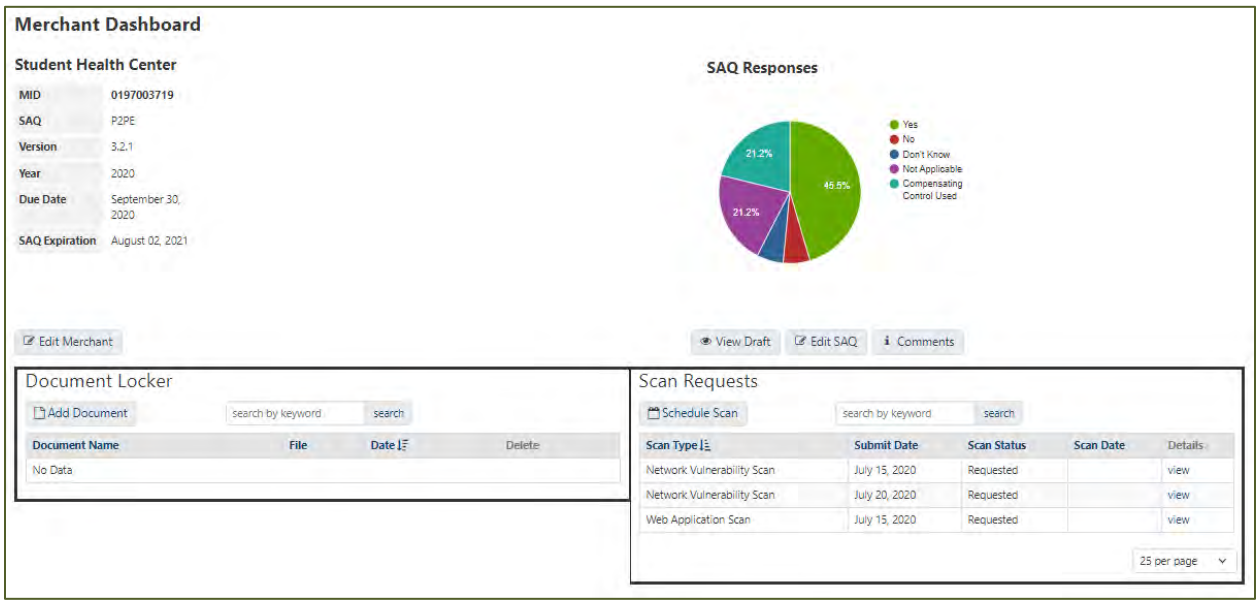


Administrator Dashboard

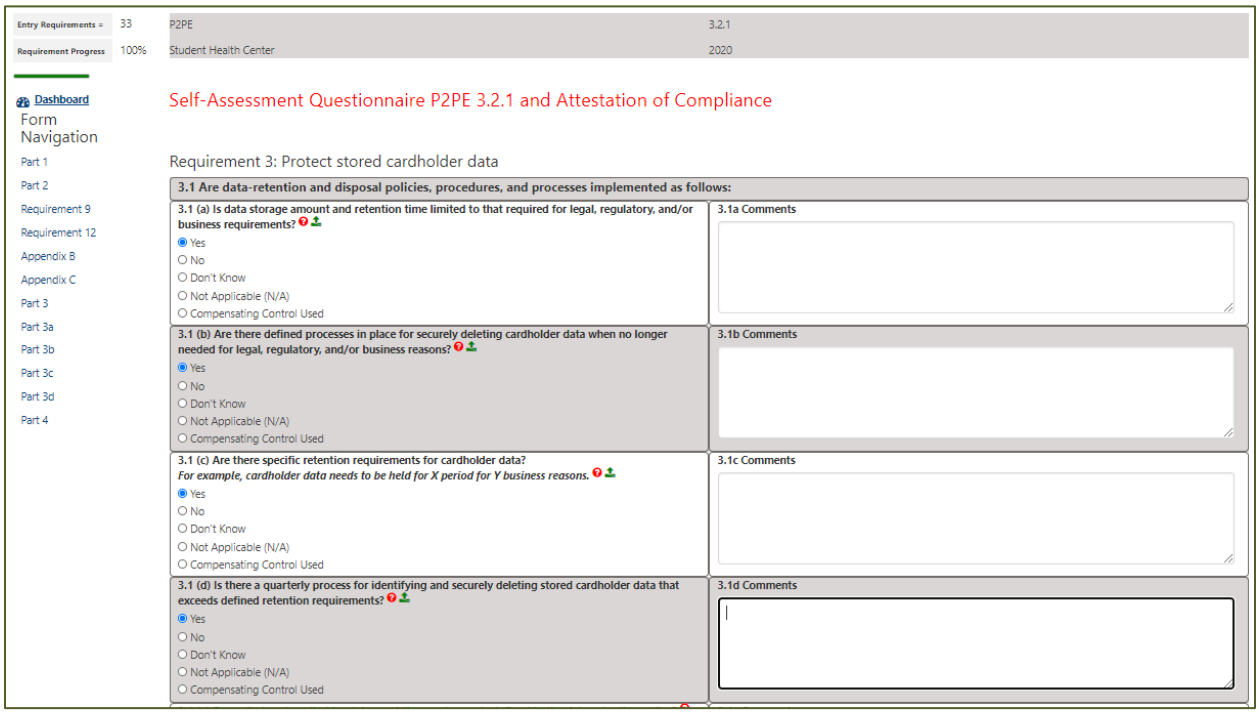


RFP Section V.B.2 and Section IV.A.1.d

Merchant Dashboard



Self-Assessment Questionnaire



RFP Section V.B.2 and Section IV.A.1

e. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Describe the dedicated QSA/customer service team that would be assigned to the University.

For all CampusGuard engagements, a Customer Advocate Team is assigned. Each team is comprised of a Customer Relationship Manager (CRM), a Security Advisor (QSA), and—when the engagement includes penetration testing—a team of penetration testers. The CampusGuard CRM will coordinate all communication closely with the University in order to develop and ensure continual oversight, and confirm the services being provided are accomplishing your goals.

The CRM will assist in the project coordination with the technical guidance coming from your QSA. The CRM will closely manage all activities and deadlines and will serve as the central point of contact for the University. In this role, the CRM will coordinate with you to set up communication preferences and regularly scheduled status update meetings.

Because our schedule is so dynamic, we cannot name those individuals at this time, but we will be happy to provide credentials and resumes at the time of being named a finalist or at the time of award.

f. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

Employee awareness goes a long way toward reducing organizational risk. The CampusGuard PCI DSS training courses were developed specifically for campus-based organizations and include three separate modules for each critical category of employee within your organization. As explained in the PCI DSS, Requirement 12.6 is important because, "*If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions*."

CampusGuard's PCI Compliance Training Bundle offers three comprehensive courses designed specifically to help employees understand their role in achieving and maintaining PCI compliance. They will learn how to identify potential risks, discuss tips, and best practices, and understand what is required to achieve PCI compliance. Each course completion certificate includes a documented annual acknowledgement of your organization's payment card policies and procedures.

PCI DSS for Merchants

The PCI DSS requires awareness training for all employees who are involved in any capacity in the processing, storing, and/or transmission of cardholder data.

RFP Section V.B.2 and Section IV.A.1.f

PCI DSS for IT Staff

The PCI for IT Staff is more technical and examines specific requirements in detail. While the merchant training discusses how to accept payment cards, identity fraud, etc., the IT training focuses more on the actual role IT plays in PCI compliance.

PCI DSS Training for Executives

The Executive Course provides a high-level overview of what the Standard is and what it means for the organization.

The online training is accessible from anywhere and allows learners to complete the course at a time that fits their schedule. This is also the perfect solution for training new hires throughout the year as they come on board, and all staff annually thereafter as required. All online training can be provided in one of two ways; either via our fully hosted, robust learning management system or delivered to you as a SCORM-compliant file for use on your internal LMS. If hosted through CampusGuard, customers have the option to receive on demand, documented progress reports so you can monitor and easily track your staff's progress. The training courses can also be customized to include organization-specific requirements, references to policy, PCI team contacts, etc.

RFP Section V.B.2 and Section IV.A.2

GLBA Consulting Services

a. Describe the firm's experience with the GLBA Safeguards within the higher education community.

Due to the experience and success CampusGuard had with PCI DSS consulting, CampusGuard made the decision to transition to a full cybersecurity and compliance consulting firm in 2015. Since that time, CampusGuard has provided hundreds of GLBA assessments to institutions of higher education and helped to build their GLBA compliance programs through ongoing consultation, remediation assistance, penetration testing, and online training.

If your organization is determined to be a "financial institution" per the Gramm-Leach-Bliley Act, CampusGuard will evaluate whether safeguards are in place to protect the confidentiality, integrity, and availability of protected data. Any organization that provides deferred payment options, including but not limited to, payment plans, loans, etc. would meet this definition. Safeguards evaluated include the following:

- A documented information security program
- Designated employee(s) to coordinate the program
- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments
- Employee training and management
- Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
- Detecting, preventing, and responding to attacks, intrusions, or other system failures
- Control the risks identified, by designing and implementing informational safeguards and regularly test/monitor their effectiveness.

The objective of a GLBA Assessment is to gauge compliance with key cybersecurity elements of the GLBA Safeguards Rule. Goals for the assessment include: the identification and analysis of risk areas, understanding the impact of third-party servicers, and evaluating the sampled areas against selected industry-recognized information security frameworks.

b. Describe the methods and processes used to ascertain compliance at a university.

CampusGuard has developed an approach and methodology that takes into consideration the standards of information security using the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171), the framework used to evaluate GLBA environments, and how to apply those standards in the higher education environment. The services described in this section include our proprietary assessment that prepares all eligible departments and the IT organization for GLBA compliance. Department and institutional policies and business processes are reviewed and reported on, a review of the networks that support them are analyzed for adherence to the NIST Framework, and third-party service

RFP Section V.B.2 and Section IV.A.2.b

providers are assessed to ensure their value and own compliance are intact. CampusGuard then delivers a detailed Final Findings Report and Roadmap that guides the organization to full compliance. Following the delivery of the Final Findings Report, remediation support and consulting can be used for any ongoing Department initiative. Using the Report, CampusGuard and the institution will work through gaps identified in the report to address and remediate vulnerabilities. Once, remediated, your dedicated Customer Relationship manager and subject matter expert team will provide continued consultation and services necessary to maintain that ongoing complaint status.

CampusGuard uses the NIST SP 800-171 due to the recommendation of the Federal Student Aid (FSA) in their follow up letter to the *Dear Colleague Letter* in July of 2016. Specifically, the NIST SP 800-171 identifies recommended requirements for ensuring the appropriate long-term security of applicable information in possession of institutions.

We will assess the University's environment to understand where the University has complied with GLBA and the new Safeguards Rules such as:

- Develop, implement, and maintain a written information security program
- Designate the employee(s) responsible for coordinating the information security program
- Continue to perform risk assessments where the assessment documents the criteria used to evaluate and categorize identified security risks
- Identify where specific safeguards have been implemented to include:
- Multifactor authentication
- Access controls
- The principle of least privilege
- Encryption
- Vulnerability scanning and penetration testing
- Data inventory and classification practices
- Change management
- Secure development practices
- Incident Response plan
- and more.
- Select appropriate service providers that are capable of maintaining appropriate safeguards
- Implement enhanced security training requirements where the training be updated based on evolving risk assessments or changes in the institution's practices

As recommended by the FSA, CampusGuard uses the NIST SP 800-171, the recognized information security publication for protecting Controlled Unclassified Information (CUI), a subset of Federal data that includes unclassified information that requires safeguarding controls consistent with law, regulation, and Federal policies.

RFP Section V.B.2 and Section IV.A.2.b

Our assessment methodology is broken up into the following phases:

Phase 1: Charter Meeting

The project is initiated with a kick-off meeting to re-state objectives and align all participants to roles and responsibilities, communication methods and schedules. The charter meeting serves to introduce all participants, establishes key dates and timelines, and discusses methodologies and tools. During this meeting, a detailed itinerary and agenda will be covered for the Assessment.

Phase 2: Information Gathering

CampusGuard will work with the University to collect the necessary documentation and evidence for the scheduled assessment.

CampusGuard will review and analyze all submitted documentation and evidence to include all policies and procedures, system configurations, and other evidence as necessary by the NIST SP 800-171. Any areas where gaps may exist shall be identified, documented, and reported to the University for appropriate action in the Final Findings Report.

Phase 3: Assessment

CampusGuard conducts the GLBA Assessment. CampusGuard will provide an experienced, certified Security Advisor to perform an assessment to validate the University's adherence to the NIST framework used. The assessment includes interviews with key IT operations personnel, department personnel (designated by both CampusGuard and the University) and review of both the IT and business environments in scope.

Phase 4: Review Information from Assessment

CampusGuard Security Advisors review all information obtained during the assessment. At the end of our engagement, we debrief the team on all pertinent activities and deliver a high-level, interim report to the Project Committee and executive-level sponsors, which identifies the highest priority risks the institution faces along with possible remediation steps.

Phase 5: Presentation of Final Findings Report

After the assessment, CampusGuard prepares a written report outlining the team's findings and recommendations. We will distribute drafts for comments and corrections and to fill in the missing information. The final report is usually ready within 20 - 30 business days of our assessment.

- CampusGuard presents findings and recommendations to the University team. We report on elements in the existing environment and security controls as evaluated against the NIST SP 800-171.
- We provide a detailed report indicating secure and non-secure areas.

RFP Section V.B.2 and Section IV.A.2.b-c

- We provide feasible, economical, and practical remedial plans to correct all gaps and recommendations of suitable compensating controls.

Strategy and Plan of Action

CampusGuard provides a Final Findings Report of elements in the existing environment and security controls as evaluated against the NIST SP 800-171 to address compliance with the new Safeguards Rule. The Final Findings Report is comprehensive, reporting on the entire environment reviewed, including each campus department included in the assessment.

Knowledge Transfer

CampusGuard believes in developing and maintaining long-term successful relationships with our customers. A significant factor in developing that type of relationship is in helping educate our clients. To reach that goal, our services are designed to be highly interactive, and we encourage your staff to be involved in all phases. This personal interaction builds staff skills and is critical to a complete understanding of our findings and advice. This approach works well to transfer knowledge to those individuals who are ultimately responsible for information security at the University.

Phase 6: Remediation

The University takes action to modify and/or change the environments based on findings described in the Findings Report. Changes may require the adjustment of existing policies and procedures, re-assessment, re-testing, etc.

Phase 7: Follow Up Consultation (ongoing after assessment)

CampusGuard provides ongoing consulting, training, vulnerability scanning, and penetration testing in partnership to assure continued compliance and security. We provide continuing guidance and ongoing support as a member of your overall project team. The partnership with the University is enhanced as CampusGuard will always be available to assist with compliance and security efforts. Also, throughout the term of the agreement, CampusGuard keeps the University up to date on the latest trends in information security and overall information about new threats that have been identified. Through your dedicated team of both a Customer Relationship Manager and Security Advisor, you will be surrounded by experts who have your best interest in mind.

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

CampusGuard has both Security Awareness Training (see IT Compliance Consulting Services) and GLBA online training modules. The GLBA training course is designed to help your organization and employees safeguard sensitive personal information and prevent potential data breaches. The training provides an overview of the GLBA Privacy Rule and Safeguards Rule, discusses relevant general cybersecurity best practices that apply to your environments under

RFP Section V.B.2 and Section IV.A.2.c-d

the GLBA, and explains the potential consequences of non-compliance. The training course will meet the primary administrative control requirement within the GLBA Safeguards Rule to provide relevant security training and maintain or increase overall awareness to all impacted employees.

The online training is accessible from anywhere and allows learners to complete the course at a time that fits their schedule. This is also the perfect solution for training new hires throughout the year as they come on board, and all staff annually thereafter as required. All online training can be provided in one of two ways; either via our fully hosted, robust learning management system or delivered to you as a SCORM-compliant file for use on your internal LMS. If hosted through CampusGuard, customers have the option to receive on demand, documented progress reports so you can monitor and easily track your staff's progress. The training courses can also be customized to include organization-specific requirements, references to policy, GLBA team contacts, etc.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

As noted above, for all CampusGuard engagements, a Customer Advocate Team is assigned. Each team is comprised of a Customer Relationship Manager (CRM), a Security Advisor, and—when the engagement includes penetration testing—a team of penetration testers. The CampusGuard CRM will coordinate all communication closely with the University in order to develop and ensure continual oversight, and confirm the services being provided are accomplishing your goals.

The CRM will assist in the project coordination with the technical guidance coming from your Security Advisor. The CRM will closely manage all activities and deadlines and will serve as the central point of contact for the University. In this role, the CRM will coordinate with you to set up communication preferences and regularly scheduled status update meetings.

Because our schedule is so dynamic, we cannot name those individuals at this time, but we will be happy to provide credentials and resumes at the time of being named a finalist or at the time of award.

RFP Section V.B.2 and Section IV.A.3

HIPAA Consulting Services

a. Describe the firm's experience with HIPAA / HITECH compliance within the higher education community.

Due to the experience and success CampusGuard had with PCI DSS consulting, CampusGuard made the decision to transition to a full cybersecurity and compliance consulting firm in 2015. Since that time, CampusGuard has provided HIPAA assessments to institutions of higher education and helped to build their HIPAA compliance programs through ongoing consultation, remediation assistance, and online training.

The Health Insurance Portability and Accountability Act (HIPAA) and subsequent Health Information Technology for Economic and Clinical Health (HITECH) Act define policies, procedures, and processes that are required to protect electronic protected health information (ePHI). As the regulatory oversight related to HIPAA increases, ensuring compliance becomes more valuable to you and your customers. CampusGuard offers comprehensive services to review safeguards to help you identify risks, meet compliance requirements, and keep up with changes. Our services enhance your information security program to include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Safeguards
- Breach Notification

Your CampusGuard team will provide strategic advice on regulatory applicability, questions of program implementation, assistance in the application of specific security documentation, and detailed assessment and validation of implemented security controls to ensure appropriate protections are in place.

b. Describe the methods and processes used to ascertain compliance at a university.

CampusGuard has developed an approach and methodology that takes into consideration the standards of information security, and how to apply different standards in the higher education environment. CampusGuard will utilize the NIST SP 800-66 for the HIPAA assessment unless otherwise asked to use another framework. CampusGuard will gather policies, procedures, and other pre-assessment information for review, conduct interviews utilizing the identified controls to ensure they are deployed properly, and deliver a detailed Findings Report that verifies the usage of these controls and where existing gaps exist requiring remediation. Using the Report, CampusGuard and the institution will work through gaps identified in the report to address and remediate vulnerabilities. Once, remediated, your dedicated Customer Relationship manager and subject matter expert team will provide continued consultation and services necessary to maintain that ongoing complaint status.

RFP Section V.B.2 and Section IV.A.3.b

The overall goals for the assessment include the following:

- Identification and verification of entities conducting covered functions
- Administration policies and procedures relating to HIPAA in all University offices and departments conducting covered functions
- Physical facility and office conditions relating to HIPAA in all University offices and departments conducting covered functions
- Information technologies related to HIPAA in all University offices and departments conducting covered functions

Phase 1: Charter Meeting

The project is initiated with a kick-off meeting to re-state objectives and align all participants to roles and responsibilities, communication methods, and schedules. The charter meeting serves to introduce all participants, establishes key dates and timelines, and discusses methodologies and tools. During this meeting, a detailed itinerary and agenda will be covered.

Phase 2: Information Gathering

CampusGuard will work with the University to collect the necessary documentation and evidence for a complete and comprehensive assessment. Documentation includes current departmental policies, procedures, and agreements. Also, we will review University policies, network diagrams of the environment(s) in scope, any additional documentation required by the controls and rules, and a list of the information systems and network environments that store, maintain, or transmit PHI/ePHI to be assessed.

CampusGuard will review and analyze all submitted documentation and evidence to include policies and procedures, the University incident response plan, standards, system configurations, and other evidence as necessary. Any areas on non-compliance shall be identified, documented, and reported to the University for remediation in the Final Findings Report.

Phase 3: Conduct Interviews

CampusGuard provides an experienced, certified Security Advisor to perform the interview portion of the assessment to validate the University's adherence to the HIPAA Privacy and Security Rules. The assessment includes interviews with key business and IT operations personnel, review of the physical environments of the offices, departments, and buildings required to comply with HIPAA regulations, and an investigation of areas potentially using PHI/ePHI within their offices and departments not currently known or documented by the University.

RFP Section V.B.2 and Section IV.A.3.b-c

Phase 4: Review Information from Interviews

CampusGuard Security Advisor reviews all information obtained during the interview portion of the assessment. At the end of the initial interview process we debrief the team on all pertinent activities and deliver a high-level, interim report to the Project Committee and executive-level sponsors, which identifies the highest priority risks the institution faces and possible remediation steps.

Phase 5: Presentation of Final Findings Report

Following the interviews, CampusGuard prepares a written report outlining the team's findings and recommendations. We will distribute drafts for comments and corrections and to fill in missing information. The final report is ready within 20-30 business days of our assessment.

- CampusGuard presents findings and recommendations to the customer team. We report on elements in the existing environment and security controls as evaluated against the NIST SP 800-66 framework.
- We provide a detailed report indicating compliant and non-compliant areas.
- We provide feasible, economical, and practical remedial plans to correct all non-compliant areas and recommendations of suitable compensating controls.

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

Health Insurance Portability and Accountability Act (HIPAA) Course Bundle

CampusGuard's HIPAA course bundle offers two comprehensive courses designed specifically to help employees understand their role in safeguarding your organization's protected health information in a compliant manner. They will learn with real-life scenarios and best practices for identifying and preventing potential exposures of health information. These courses explain what information is protected, outline the organizations and entities that are subject to HIPAA, provide an overview of compliance with both the Privacy and Security rules, and review the consequences of non-compliance.

HIPAA for Administrators

Periodic training for all employees who are involved in any capacity in the processing, storing, and/or transmission of protected health information (PHI) is required according to the HIPAA Privacy and Security Rules. Empower your staff with ongoing awareness and best practices for protecting and limiting access to PHI ongoing.

HIPAA for Staff

The HIPAA for Administrators course provides a high-level overview of the specific requirements that apply to your organization and outlines the administrative controls that must be in place to ensure ongoing compliance.

RFP Section V.B.2 and Section IV.A.3.c-d

The online training is accessible from anywhere and allows learners to complete the course at a time that fits their schedule. This is also the perfect solution for training new hires throughout the year as they come on board, and all staff annually thereafter as required. All online training can be provided in one of two ways; either via our fully hosted, robust learning management system or delivered to you as a SCORM-compliant file for use on your internal LMS. If hosted through CampusGuard, customers have the option to receive on demand, documented progress reports so you can monitor and easily track your staff's progress. The training courses can also be customized to include organization-specific requirements, references to policy, HIPAA team contacts, etc.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

As noted above, for all CampusGuard engagements, a Customer Advocate Team is assigned. Each team is comprised of a Customer Relationship Manager (CRM), a Security Advisor, and—when the engagement includes penetration testing—a team of penetration testers. The CampusGuard CRM will coordinate all communication closely with the University in order to develop and ensure continual oversight, and confirm the services being provided are accomplishing your goals.

The CRM will assist in the project coordination with the technical guidance coming from your Security Advisor. The CRM will closely manage all activities and deadlines and will serve as the central point of contact for the University. In this role, the CRM will coordinate with you to set up communication preferences and regularly scheduled status update meetings.

Because our schedule is so dynamic, we cannot name those individuals at this time, but we will be happy to provide credentials and resumes at the time of being named a finalist or at the time of award.

RFP Section V.B.2 and Section IV.A.4

FERPA Consulting Services

a. Describe the firm's experience with FERPA within the higher education community.

Due to the experience and success CampusGuard had with PCI DSS consulting, CampusGuard made the decision to transition to a full cybersecurity and compliance consulting firm in 2015. Since that time, CampusGuard has provided FERPA assessments to institutions of higher education and helped to build their FERPA compliance programs through ongoing consultation, remediation assistance, and online training.

FERPA is a federal law that protects the privacy and confidentiality of student educational records. Once a student reaches 18 years of age or attends a postsecondary institution, they become an "eligible student," and all rights formerly given to parents under FERPA transfer to the student. The objective of the CampusGuard FERPA services is to determine the gaps in compliance with critical cybersecurity requirements of protected information.

Your CampusGuard team will provide strategic advice on regulatory applicability, questions of program implementation, assistance in the application of specific security documentation, and detailed assessment and validation of implemented security controls to ensure appropriate protections are in place.

b. Describe the methods and processes used to ascertain compliance at a university.

CampusGuard has developed an approach and methodology that takes into consideration the standards of information security using the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) or other framework as desired by the institution, and how to apply those standards in the higher education environment. The services described in this section include our proprietary assessment that prepares all eligible departments and the IT organization for FERPA compliance. Department and institutional policies and business processes are reviewed and reported on, a review of the networks that support them are analyzed for adherence to the NIST Framework, and third-party service providers are assessed to ensure their value and own compliance are intact. CampusGuard then delivers a detailed Final Findings Report and Roadmap that guides the organization to full compliance. Using the Report, CampusGuard and the institution will work through gaps identified in the report to address and remediate vulnerabilities. Once, remediated, your dedicated Customer Relationship manager and subject matter expert team will provide continued consultation and services necessary to maintain that ongoing complaint status. We will assess the University's environment to understand where the University has complied with the FERPA such as:

- How the University produces requests of educational data for parents, legal guardians, or students within appropriate timelines.
- How the University amends records as requested.

RFP Section V.B.2 and Section IV.A.4.b

- How the University reminds parents/legal guardians and students of their rights under FERPA on an annual basis.
- Barring certain exceptions, the University does not share an eligible student's education records without the written consent of the parent or legal guardian – or, if they are of age, the student themselves.

Our assessment methodology is broken up into the following phases:

Phase 1: Charter Meeting

The project is initiated with a kick-off meeting to re-state objectives and align all participants to roles and responsibilities, communication methods and schedules. The charter meeting serves to introduce all participants, establishes key dates and timelines, and discusses methodologies and tools. During this meeting, a detailed itinerary and agenda will be covered for the Assessment.

Phase 2: Information Gathering

CampusGuard will work with the University to collect the necessary documentation and evidence for the scheduled assessment.

CampusGuard will review and analyze all submitted documentation and evidence to include all policies and procedures, system configurations, and other evidence as necessary by the NIST SP 800-171 (or other framework). Any areas where gaps may exist shall be identified, documented, and reported to the University for appropriate action in the Final Findings Report.

Phase 3: Assessment

CampusGuard conducts the FERPA Assessment. CampusGuard will provide an experienced, certified Security Advisor to perform an assessment to validate the University's adherence to the NIST framework used. The assessment includes interviews with key IT operations personnel, department personnel (designated by both CampusGuard and the University) and review of both the IT and business environments in scope.

Phase 4: Review Information from Assessment

CampusGuard Security Advisors review all information obtained during the assessment. At the end of our engagement, we debrief the team on all pertinent activities and deliver a high-level, interim report to the Project Committee and executive-level sponsors, which identifies the highest priority risks the institution faces along with possible remediation steps.

Phase 5: Presentation of Final Findings Report

After the assessment, CampusGuard prepares a written report outlining the team's findings and recommendations. We will distribute drafts for comments and corrections and to fill in the missing information. The final report is usually ready within 20- 30 business days of our assessment.

RFP Section V.B.2 and Section IV.A.4.b

- CampusGuard presents findings and recommendations to the institutional team. We report on elements in the existing environment and security controls as evaluated against the NIST Framework.
- We provide a detailed report indicating secure and non-secure areas.
- We provide feasible, economical, and practical remedial plans to correct all gaps and recommendations of suitable compensating controls.

Strategy and Plan of Action

CampusGuard provides a Final Findings Report of elements in the existing environment and security controls as evaluated against the NIST Framework. The Final Findings Report is comprehensive, reporting on the entire environment reviewed, including each campus department included in the assessment.

Knowledge Transfer

CampusGuard believes in developing and maintaining long-term successful relationships with our customers. A significant factor in developing that type of relationship is in helping educate our clients. To reach that goal, our services are designed to be highly interactive, and we encourage your staff to be involved in all phases. This personal interaction builds staff skills and is critical to a complete understanding of our findings and advice. This approach works well to transfer knowledge to those individuals who are ultimately responsible for information security at the University.

Phase 6: Remediation

The University takes action to modify and/or change the environments based on findings described in the Findings Report. Changes may require the adjustment of existing policies and procedures, re-assessment, re-testing, etc.

Phase 7: Follow Up Consultation (ongoing after assessment)

CampusGuard provides ongoing consulting, training, vulnerability scanning, and penetration testing in partnership to assure continued compliance and security. We provide continuing guidance and ongoing support as a member of your overall project team. The partnership with the University is enhanced as CampusGuard will always be available to assist with compliance and security efforts. Also, throughout the term of the agreement, CampusGuard keeps the University up to date on the latest trends in information security and overall information about new threats that have been identified. Through your dedicated team of both a Customer Relationship Manager and Security Advisor, you will be surrounded by experts who have your best interest in mind.

RFP Section V.B.2 and Section IV.A.4

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

The FERPA online training course helps your institution safeguard sensitive student information in a compliant manner and prevent potential data breaches. This course provides an overview of the laws governing acceptable use and release of student records, discusses individual staff and faculty responsibilities, provides guidance on how to protect students' right to privacy, and explains the potential consequences of non-compliance. Users will walk through common campus scenarios and requests for student information and learn how to avoid potential exposures of data.

The online training is accessible from anywhere and allows learners to complete the course at a time that fits their schedule. This is also the perfect solution for training new hires throughout the year as they come on board, and all staff annually thereafter as required. All online training can be provided in one of two ways; either via our fully hosted, robust learning management system or delivered to you as a SCORM-compliant file for use on your internal LMS. If hosted through CampusGuard, customers have the option to receive on demand, documented progress reports so you can monitor and easily track your staff's progress. The training courses can also be customized to include organization-specific requirements, references to policy, FERPA team contacts, etc.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

As noted above, for all CampusGuard engagements, a Customer Advocate Team is assigned. Each team is comprised of a Customer Relationship Manager (CRM), a Security Advisor, and—when the engagement includes penetration testing—a team of penetration testers. The CampusGuard CRM will coordinate all communication closely with the University in order to develop and ensure continual oversight, and confirm the services being provided are accomplishing your goals.

The CRM will assist in the project coordination with the technical guidance coming from your Security Advisor. The CRM will closely manage all activities and deadlines and will serve as the central point of contact for the University. In this role, the CRM will coordinate with you to set up communication preferences and regularly scheduled status update meetings.

Because our schedule is so dynamic, we cannot name those individuals at this time, but we will be happy to provide credentials and resumes at the time of being named a finalist or at the time of award.

RFP Section V.B.2 and Section IV.A.5

IT Compliance Consulting Services

a. Describe the firm's experience with NIST 800-171 and ISO 27001 within the higher education community.

CampusGuard has over 13 years of experience and has partnered with over 400 customers to assist in successfully establishing secure information technology security infrastructures and procedures to protect confidential and sensitive information. We execute our services with highly qualified personnel who have extensive experience and are provided up-to-date tools with which to work.

CampusGuard has collaborated with hundreds of campus-based organizations to assist in successfully establishing secure information technology security infrastructures and procedures to protect confidential and sensitive information. We use a number of NIST frameworks at our customers' request, including the NIST SP 800-53, NIST SP 800-171, and the NIST CSF. We also are familiar with other frameworks and standards as they apply to other security and compliance initiatives and will use that experience throughout any engagement.

CampusGuard will assess whether operations and senior management have identified, measured, controlled, and monitored information technology to avoid gaps that threaten the safety and soundness of the organization and provide summary and detailed level reporting to map out best practices and a path to a secure environment.

CampusGuard will assess that the organization has plans for use of technology, assessed the risk associated with technology, decided how to implement the technology, and established a formal process to measure and monitor identified gaps.

We will also assess that the organization has an effective planning process that aligns IT and business objectives, an ongoing assessment process that evaluates the environment and potential changes, technology implementation procedures that include appropriate controls, and measurement and monitoring efforts that effectively identify ways to manage exposure.

b. Describe the methods and processes used to assist the university to adhere to the standards.

CampusGuard has developed an approach and methodology that takes into consideration the standards of information security and how to apply different standards in the campus-based environment. For customers like the University, where an established set of information security roles and responsibilities are being developed, CampusGuard will use the appropriate framework to assess the environment from an external viewpoint. For many general cybersecurity assessments, CampusGuard uses the NIST Cybersecurity Framework as the set of controls in which to evaluate the identified environment. CampusGuard will collect and review documentation, conduct interviews utilizing the agreed upon Framework to ensure they are appropriately deployed, review network topography, and deliver a detailed Final Findings Report that verifies the usage of these controls and where existing gaps reside requiring remediation. Using the Report, CampusGuard and the institution will work through gaps

RFP Section V.B.2 and Section IV.A.5.b

identified in the report to address and remediate vulnerabilities. Once, remediated, your dedicated Customer Relationship manager and subject matter expert team will provide continued consultation and services necessary to maintain that ongoing complaint status.

Our assessment methodology is broken up into the following phases:

Phase 1: Charter Meeting

The project is initiated with a kick-off meeting that restates objectives and aligns all participants to roles and responsibilities, communication methods, and schedules. The charter meeting serves to get all participants introduced, establishes key dates and timelines, and discusses methodologies and tools. During this meeting, a detailed itinerary and agenda will be covered.

Phase 2: Information Gathering

CampusGuard will work with the University to collect the necessary documentation and evidence for the scheduled assessment.

CampusGuard will review and analyze all submitted documentation and evidence to include all policies and procedures, system configurations, network topography, and other evidence as necessary by the security controls used. Any areas where gaps may exist shall be identified, documented, and reported to the University for appropriate action in the Final Findings Report.

Phase 3: Conduct Assessment

CampusGuard conducts the assessment and will provide an experienced, certified Security Advisor to perform an assessment to validate the University's adherence to the NIST controls. The assessment includes interviews with key business and IT operations personnel and review of the environment and remaining documentation in scope. The assessment will include a review of the below NIST CSF functions, their categories, subcategories, and how they have been deployed in their respective environments.

- Identify
- Protect
- Detect
- Respond
- Recover

Phase 4: Review Information from Site Visit

CampusGuard Security Advisors review all information obtained during the assessment. At the end of our engagement, we debrief the team on all pertinent activities and deliver a high-level, interim report to the executive-level sponsors, which identifies the highest priority risks the organization faces and possible remediation steps.

RFP Section V.B.2 and Section IV.A.5.b

Phase 5: Presentation of Final Findings Report

After the assessment, CampusGuard prepares a written report outlining the team's findings and recommendations. We will distribute drafts for comments and corrections and to fill in missing information. The final report is usually ready within 20 business days of our assessment.

- CampusGuard presents findings and recommendations to the customer team. We report on elements in the existing environment and security controls as evaluated against the specific requirements within the NIST Cybersecurity Framework.
- We provide a detailed report indicating compliant and non-compliant areas.
- We provide feasible, economical, and practical remedial plans to correct all non-compliant areas and recommendations of suitable compensating controls.

Strategy and Plan of Action

CampusGuard provides a Final Findings Report of elements in the existing environment and security controls as evaluated against the specific requirements of the NIST CSF. The Final Findings Report is comprehensive, reporting on the entire environment reviewed, including each location and the departments interviewed.

Knowledge Transfer

CampusGuard believes in developing and maintaining long-term successful relationships with our customers. A major factor in developing that type of relationship is in helping educate our clients. To reach that goal, our services are designed to be highly interactive, and we encourage your staff to be involved in all phases. This personal interaction builds staff skills and is critical to complete understanding of our findings and advice. This approach works well to transfer knowledge to those individuals who are ultimately responsible for information security.

Phase 6: Remediation

The University takes action to modify and/or change the environments based on findings described in the Findings Report. Changes may require the adjustment of existing policies and procedures, re-assessment, re-testing, etc.

Phase 7: Remediation Consultation (following assessment)

CampusGuard provides several ongoing consulting and remediation services in partnership to assure continued organizational security. We provide continuing guidance and ongoing support as a member of your overall project team. The partnership with the University is enhanced as CampusGuard will always be available to assist with security efforts. In addition, throughout the term of the agreement, CampusGuard keeps the University up to date on the latest trends in information security and overall information about new threats that have been identified. Through your dedicated team of both a Customer Relationship Manager and Security Advisor, you will be surrounded by experts who have your best interest in mind.

RFP Section V.B.2 and Section IV.A.5

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

Security Awareness Training

Employees are the most important asset in your organization, but they can also be the weakest link in your information security program. Security Awareness Training is a required element of any security program strategy. Training should address common threats such as phishing, email, web browsing, social engineering, social networking, Wi-Fi, and information protection. End users should be educated as to how to utilize assets in a secure manner by using the VPN, encryption, and secure communications.

CampusGuard's courses are designed to empower your staff with awareness and provide all employees and third parties with access to your organization's computer systems, networks, and information with the knowledge to protect and reduce the risk to sensitive information. The online training is accessible from anywhere and allows learners to complete the course at a time that fits their schedule. This is also the perfect solution for training new hires throughout the year as they come on board, and all staff annually thereafter as required. All online training can be provided in one of two ways; either via our fully hosted, robust learning management system or delivered to you as a SCORM-compliant file for use on your internal LMS. If hosted through CampusGuard, customers have the option to receive on demand, documented progress reports so you can monitor and easily track your staff's progress.

Information Security Awareness Course

Employees remain the weakest link in information security. Criminals are finding that it is much easier to hack a person than it is to bypass organizational security technologies. It is critical to incorporate your employees into your ongoing security awareness program and motivate them to implement information security best practices into their daily roles and responsibilities.

The CampusGuard Information Security Awareness Course is based on industry-standard information security best practices and align with many major standards, including NIST, ISO/IEC, and PCI, to name a few. Our comprehensive Information Security Awareness course is intended for all employees and third parties with access to your organization's computer systems, networks, and information. The course provides these key personnel with the knowledge to protect and reduce the risk to sensitive information on an ongoing basis.

Phishing/Spear Phishing Course

Phishing continues to be the most common cyberattack vector and is often determined to be the initial point of compromise in large scale data breaches. As an organization, it is critical to provide your staff and employees with the tools to proactively identify potential phishing emails and prevent the accidental disclosure of sensitive information. CampusGuard's phishing training, whether used as supplemental training to your current security awareness program, or as targeted training for staff as part of your ongoing phishing simulations, will help users

strengthen their ongoing awareness. The modules will walk learners through common goals and strategies used within phishing campaigns, teach them how to identify red flags and phishing indicators within email messages, and provide your staff with best practices for protecting themselves, as well as your organization, from data compromises.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

As noted above, for all CampusGuard engagements, a Customer Advocate Team is assigned. Each team is comprised of a Customer Relationship Manager (CRM), a Security Advisor, and—when the engagement includes penetration testing—a team of penetration testers. The CampusGuard CRM will coordinate all communication closely with the University in order to develop and ensure continual oversight, and confirm the services being provided are accomplishing your goals.

The CRM will assist in the project coordination with the technical guidance coming from your Security Advisor. The CRM will closely manage all activities and deadlines and will serve as the central point of contact for the University. In this role, the CRM will coordinate with you to set up communication preferences and regularly scheduled status update meetings.

Because our schedule is so dynamic, we cannot name those individuals at this time, but we will be happy to provide credentials and resumes at the time of being named a finalist or at the time of award.

e. Describe other technology-related consulting services available from your firm.

Other CampusGuard technology-related consulting services include:

Vulnerability Scanning and Penetration Testing

CampusGuard's scanning and testing methodology reflects industry best practices, OWASP and NIST. We closely follow the NIST 800-115 penetration testing methodology and the PCI DSS penetration testing guidance. By using an established, proven, and industry-standard methodologies, CampusGuard is able to complete testing efficiently and effectively. The following paragraphs outline the CampusGuard methodology for our vulnerability scanning and penetration testing functions.

Vulnerability Scanning

A key aspect of any security program is the ability to manage vulnerabilities. This involves assessing, mitigating (when necessary), and reporting on security vulnerabilities that exist in an organization's networks, systems, and software. To effectively manage this process, an organization must have a vulnerability management program in place to identify potential exposures.

RFP Section V.B.2 and Section IV.A.5.e

The CampusGuard vulnerability scanning service scans networks, systems, and software from an attacker's point of view. We use industry-standard automated and manual scanning tools that have been well tested to discover vulnerabilities such as deficiencies in patch management, the use of weak protocols or services, and misconfigurations that could lead to information leakage on the customer's systems. These tools contain vast libraries of checks to ensure that present vulnerabilities are appropriately identified.

All organizations will have vulnerabilities; our reports include remediation instructions that are prioritized by severity and frequency so that customer resources can be efficiently allocated and managed. CampusGuard will ensure the member organization understands the ratings of any discovered vulnerabilities using the Common Vulnerabilities and Exposures (CVE) rating system. CampusGuard will also recommend best practices based on our experience to improve the overall risk profile of the customer.

External Vulnerability Assessment

CampusGuard's external vulnerability scanning service is used to detect vulnerabilities in the perimeter defenses and external-facing systems. Information will be gathered by interviews as well as automated and manual vulnerability scanning tools. This information will be used to formulate a plan of action to test external network and host-based vulnerabilities. Audits of software and systems will be compared against documented standards (NIST, OWASP, etc.) to check for software bugs, patch levels, configurations, use of vendor supplied default settings, installed software, etc.

Well-known network and host vulnerabilities will be identified using multiple commercial tools such as Qualys' QualysGuard and Tenable's Nessus vulnerability scanner as well as open-source tools such as nmap, Metasploit, and WebScarab. The customer will help dictate the level of invasiveness of the scans. Scans can be configured to run in a passive mode or run hostile attacks during testing. Information captured by these tools can range from publicly available information (such as DNS records) to sensitive information (if configuration/misconfiguration allows for database record dumping or other data collection).

CampusGuard will scan host IP addresses from an external attacker point of view using filtering or blocking identical to any other Internet IP addresses utilizing all means available to discover potential means of access. Scanning activity will include automated scanning tools, port scans, and/or manual tools to discover vulnerabilities such as deficiencies in patch management, outdated virus and malware protection, misconfigurations that could lead to information leakage and other vulnerabilities that could allow a compromise of the systems.

RFP Section V.B.2 and Section IV.A.5.e

Internal Vulnerability Assessment

Vulnerability scans will be conducted on all in-scope devices. Configurations of systems will be reviewed and benchmarked against industry standard system hardening guidelines.

CampusGuard will scan systems from testing host IP addresses with unrestricted access at Internet borders, or scans from a testing source inside the Internet border utilizing all means available to discover potential means of access. Included are automated scanning tools, port scans and/or manual tools to discover vulnerabilities such as deficiencies in patch management, outdated virus and malware protection, misconfigurations that could lead to information leakage on systems and other vulnerabilities that could allow a compromise of the system, gain access to them and the data within.

CampusGuard's internal vulnerability scanning service will assess and detect vulnerabilities across the internal network. Our scanning tools support a wide range of devices, operating systems, databases, and applications across physical, virtual, and cloud infrastructure. Performed from behind the various firewalls, we offer options for credentialed and non-credentialed scans, threat detection, and compliance templates to simplify reporting and help ensure networks and data are secure from emerging threats.

Penetration Testing

Penetration testing involves simulating an actual attack on the customer's network to test the effectiveness of the organization's investment in security defenses. This type of testing helps to determine what a malicious person may accomplish in a real-world hacking effort. The goal of the penetration test is to ensure the best security posture for the customer through the discovery of vulnerabilities that may affect the confidentiality, integrity, and availability of the customer's data.

CampusGuard provides a penetration testing service designed to include the following:

- **Enumeration:** A list of targeted and authorized IP addresses will be developed based on customer-provided data (domain names, network blocks, and individual IP addresses). This includes intelligent domain name resolution in which dynamic, periodic name resolution is employed to discover load-balancing architectures that utilize multiple IP addresses.
- **Inventory:** CampusGuard determines which of the enumerated IP addresses are actually running, available, and offering network services. Host inventory uses several techniques, including ICMP pings, common TCP service probes, and protocol-specific service probes. In local, LAN-based scans, ARP queries also reveal active systems. Open services are probed by CampusGuard for any information that can be used to verify the actual application layer protocol (e.g., HTTP), as well as vendor applications (e.g., Apache, IIS, Netscape, Domino) and version.

RFP Section V.B.2 and Section IV.A.5.e

- **System Discovery:** CampusGuard will attempt to identify other IP addresses associated with the target IP address. Typical discovery methods include DNS record lockups and various dynamic port mapping techniques (e.g., DCE Endpoint Mapping and Java RMI Registry probes).
- **Vulnerability Checks:** CampusGuard performs specific checks for vulnerabilities on all accessible IP addresses and services within the scope of the test. Network-layer penetration tests, as well as application-layer penetration tests, should be performed. This should include Web Application Vulnerability scans that cover at a minimum the OWASP top 10.
- **Manual Analysis and Verification:** CampusGuard conducts a manual verification and analysis of the discovered vulnerabilities on systems within the scope of the test to identify security vulnerabilities, eliminates false positives, and assess the risk introduced by confirmed vulnerabilities. Upon completion of the testing, a report is provided by CampusGuard documenting the findings, including recommendations for remediation. All testing phases are coordinated with the customer to minimize any adverse impact that may occur as a result of the services.

Some tools employed by CampusGuard include the following:

- Kali Linux
- Wireshark
- Unicornscan
- Nbtscan
- Sqlmap
- Wpscan & whatweb
- Hashcat, John the Ripper, Hydra, & Medusa
- Metasploit
- Nmap/Zenmap
- Enum4linux
- SSLScan, sslsniff, & sslyze
- Snmpcheck & onesixtyone
- Nikto & skipfish
- Burp Suite, OWASP Zap, & Dirbuster
- Netcat
- Nessus Professional
- Manual methods of information gathering and parameter/packet manipulation

Rules of Engagement

Based on the customer's requirements and the information available, CampusGuard will use a white, grey, or black box methodology. CampusGuard will use the given information and vulnerability scans to perform reconnaissance and gain further knowledge of the network environment.

We tend to favor a “white box” or “grey box” approach when penetration testing. We do this for two reasons. A true emulation of advanced persistent threat groups takes time, in some cases years to collect the data and sit by patiently to allow employees to make mistakes. Knowing there is a limited amount of time to complete this project we will require a nominal amount of information to get started and not use those hours scanning, researching, and using various methods of social engineering to collect data to use during testing. The second reason comes down to money and deliverables. The more information

we have up front, the less time we need to use hours in discovery. This allows us to apply our manual methods to the appropriate testing attributes to identify those gaps in the attack surface that the customer relies on us to discover to eliminate potential threats and any negative consequences. Our penetration testing services follow a 10% automated tool-based approach and a 90% manual testing approach. This has proven to be the exact formula we need for a successful penetration testing engagement.

CampusGuard takes the results from the scanning and reconnaissance discovery and attempts to gain access/elevated privilege on the systems using well-known attacks and/or taking advantage of well-known exploits.

All information gathered will be used to attempt to gain access and/or elevated privilege on the systems and testing phases are coordinated with the customer to minimize any adverse impact that may occur as a result of the testing.

If any evidence of intrusion by a third-party is discovered during testing, CampusGuard will cease testing and will notify the customer immediately via the contact information provided. CampusGuard will also provide details in an interim status report.

In the event that CampusGuard can breach system security, CampusGuard will ensure that care is taken to not alter or damage the organization's data. Details of the breach will be documented in an interim report. CampusGuard will immediately notify the customer via the contact information provided if the breach poses significant risk to the organization's data.

Methodology

The penetration testing project plan proceeds through six phases:

Prerequisites

- An executed confidentiality agreement
- Written permission to test devices
- A brief summary of the application

Discovery

Typical discovery methods can include:

- Port scanning
- IP / Domain name lookup
- Search engine-based reconnaissance
- Identify system and/or application access prompts
- Find cookies
- Crawl the web application(s)

Creation of Attack Plan

- Enumeration: A list of targeted and authorized IP addresses and domain names will be developed based on customer-provided data
- Network diagrams and results of previous tests (if applicable)
- A list of active IP addresses
- Coordinated scan activity plan
- After-hours emergency contact information
- A secure communications method for information exchange
- Valid backups for all in-scope elements

Attack Execution

Following mutually agreed scope and rules-of-engagement, CampusGuard will perform a penetration test on all in-scope systems, applications, and/or devices.

Sampling may be used to reduce the number of devices being testing if they can be demonstrated as being identically configured (e.g., identically configured web servers behind a load balancer).

Analysis & Verification

CampusGuard conducts a manual analysis and verification of the identified findings to confirm security vulnerabilities, eliminates false positives, and assess the potential risk. Any discovered element(s) will be included in documentation, reports, and diagrams.

Creation and Delivery of Final Report

The final report will include an Executive Summary, logs of the testing, and all significant, non-remediated vulnerabilities as well as targeted recommendations for remediation.

Web Application Penetration Testing

Exploits for commonly known vulnerabilities and misconfigurations will be used to try to gain unauthorized access to the identified web applications. A vulnerability scan may be conducted first to detect vulnerabilities.

Methodology

CampusGuard will scan web applications for well-known coding vulnerabilities (e.g., injection attacks, cross-site scripting), vulnerable/unpatched server software and/or misconfigurations using automated scanning tools, web proxies and/or manual tools that could lead to information leakage or compromise of systems.

Web Application penetration testing will attempt to identify weaknesses in an application that will allow an attacker to perform unintended actions. These actions may include escalation of privileges, discovery of sensitive information, remote code execution, session

manipulation, authentication bypassing and others. Testing entails multiple facets depending on the needs of the customer. CampusGuard will perform automated and/or manual scans, both internally and externally, if necessary, to detect potential vulnerabilities and employ tools to exploit those vulnerabilities to see if a system can be compromised. A penetration test can also entail the use of social engineering to try and manipulate staff to check for their understanding and adherence to security policy and procedures.

Rules of Engagement

A white, grey, or black box testing methodology will be used to conduct the penetration test. Institutional information (such as application credentials) will be requested prior to the start of testing.

No unusual or major network changes will purposely be made by CampusGuard during testing.

If any evidence of intrusion by a third party is discovered during testing, CampusGuard will cease testing and will notify the customer immediately via the contact information provided. CampusGuard will also provide details in an interim status report.

In the event that CampusGuard can breach system security, CampusGuard will ensure that care is taken to not alter or damage any data. Details of the breach will be documented in an interim report. CampusGuard may immediately notify the organization via the contact information provided if the breach poses significant risk to the customer data.

Wireless Penetration Testing

CampusGuard's approach to wireless network security includes both high-level and detail-oriented assessments to discover and expose potential flaws in the structure, placements, and configurations in the network. A typical beginning is to review the network devices currently in place and your internal systems to determine the level of security and exposure.

Testing will include the use of automated tools and manual methods of discovery within and around the approved campuses to identify wireless networks and their broadcasted configurations, and tests will be conducted using various tools to see whether the networks are penetrable. If authentication data is obtained during testing, CampusGuard will attempt to recover plaintext credentials or keys used to gain access to the network.

We will provide details specific to the engagement methodology and documented details of any findings, as well as recommendations for remediation. We include evidence of controls, information sufficient to replicate the results, base recommendations on these root causes, and prioritize risk-based remediation with an estimation of relative work effort. Additionally, we describe strong controls in place that have been identified, as well as their impact on the customer.

RFP Section V.B.2 and Section IV.A.5.e

Engagement data may be stored on CampusGuard equipment. One or more of the following controls will be used to protect the data, depending on physical location and of the equipment used: physical security controls, whole disk encryption, multifactor authentication, VPN-tunneling, access restriction to only authorized personnel and systems.

A detailed, actionable Report of Findings will be delivered, and a Report Review call will be scheduled. Additional support hours are included to assist with remediation.

Social Engineering

While many methods are employed to test technology and networks, the only way to effectively test any organization's behavioral and operational integrity is through social engineering assessment. Social engineering is the manipulation of people and the environment to steal valuable information or to obtain services by means of identity theft. A type of confidence trick for the purpose of information gathering, fraud, or system access, often times is the first step of numerous steps in a more complex fraud scheme. When social engineering assessments are executed properly, risk managers are able to evaluate and mitigate forced breaches in a controlled environment.

Scope

To support our customer requirements, CampusGuard will engage in a series of social engineering attacks against the institution's IT infrastructure. CampusGuard will actively manipulate people and the environment to acquire valuable information or to obtain services by means of identity theft. A series of techniques will be executed across the environment with the following objectives:

- Can the hacker trick the helpdesk (or department) staff into resetting their password (or other service change)? (Pretending to be a staff member or faculty member)
- Can the hacker gain privileged access to a PC through social engineering?
- Can the hacker gain access to privileged areas through social engineering? (Server room, business offices) (for onsite assessments only)
- Can the hacker gain access to confidential and sensitive information through social engineering?

Methodology

The methods used by CampusGuard are the same tactics currently being employed by hackers. They will coerce employees into giving up valuable information. That information will be used to gain access to services or restricted areas. Social engineering tactics can include:

- Coercion
- Pre-texting
- Phishing
- Name Dropping
- Piggy Backing / Tailgating
- Dumpster Diving
- Trespassing
- Eaves Dropping
- Water Holing
- Baiting

- Password Auditing / Password Spraying

RFP Section V.B.2 and Section IV.A.5.e

Example 1: Phishing

A popular type of social engineering, Phishing is the attempt to gain sensitive information from unsuspecting employees such as usernames, passwords, social security numbers, or credit card information, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication or phone phishing. Done via email, rogue interactive voice response (IVR) systems or by human interaction, CampusGuard uses phishing experiments to test your organization's security awareness program and how your users respond to these types of attacks.

CampusGuard will work directly with our customer's security team to build a multi-step phishing campaign that incorporates both email and phone phishing. CampusGuard will construct one or more email message(s) targeting organizational employees asking for specific information or directing them to an erroneous website where CampusGuard will capture information based on user input. All information requested will be approved by member organizations prior to the start of our phishing campaign.

In addition, CampusGuard will construct a phone script to be used in an attempt to gather additional sensitive information from targeted employees. The script to be used in the phone attacks will again be vetted by member organizations prior to any attempts made on employees.

- Primary Goals - For Metrics or For Access
  - Receive metrics based on how many users click a link, open a file, or submit information after receiving a phishing email
  - Large number of users are targeted with same email (depending on environment, emails may get rejected from spam filter)
  - Receive metrics based on how many users provide answers to random phone calls inquiring about sensitive information on any number of topics previously discussed between CampusGuard and our customer.
  - Secondary goals could include assess spam filtering software, assess email configurations, assess user awareness of obvious spam and phishing techniques, and test IT's response to reported phishing attempts.
- Advanced Measures - Employed upon request and based on customer goals
  - Spear phishing will be employed to target specific users (executives, administrators, etc.)
  - Gaining access to SMTP server to send emails from internal email addresses
  - Goals could include but not be limited to testing users' knowledge of advanced phishing techniques

RFP Section V.B.2 and Section IV.A.5.e

Example 2: Password Auditing

Weak passwords are as dangerous as leaving the front door open to an attacker. Most users undergo some type of annual training, which may or may not cover the topic of choosing strong passwords. Most websites or organizational policies will require users to select passwords that meet a particular set of requirements: Be a minimum of eight characters in length, contain at least one upper case, one lower case, one number (possibly even one special character). Sounds familiar? Often times, even with restrictive password requirements, users will choose an easy-to-remember password. If those passwords are easy to remember, it is a good chance that they are easy to guess, too. The CampusGuard Offensive Security Team utilizes custom-built in-house tools to gather user account information and test authentication using uniquely generated password lists and most commonly used passwords in an attempt to identify weak passwords before an attacker does. Each password audit is highly customized to meet your needs and goals.

Incident Response Plan (IRP) Development and Testing

CampusGuard will compare current documented policy and procedures for your incident response program and test the knowledge of the staff who have responsibility and compare to the information security standard currently in place.

If no plan has been formally documented, CampusGuard has an incident response template that institutions can use to begin their incident documentation. Following the structured template completion, CampusGuard provides written recommendations for any changes required to meet the information security standards to be used according to best practice.

CampusGuard will review, at a minimum, the roles, responsibilities, and methods of communication in the event of a data compromise including notification of required parties. This will include a review of:

- The organizational incident response procedures
- Data backup process
- Analysis of legal requirements for reporting data compromises
- Coverage and responses of all critical system components
- Is the plan reviewed and tested at least once annually?
- Review of training provided
- Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?

Once developed, testing your incident response plan allows you to ensure that it is designed well and that it will cover all steps to contain the incident if you ever have to use it. To test your plan, CampusGuard will provide the external expert, one of our credentialed Security Advisors, and the scenarios to conduct tabletop exercises. This engagement can be run over the course of a full day or more and the scenarios can be shared ahead of time or presented at the time of testing. Bringing in an outside expert to run through a variety of scenarios can bring to light

RFP Section V.B.2 and Section IV.A.5.e

some previously invisible gaps. The IRP should be tested at least annually and any time there are significant changes to your environment.

Technical and Operational Policy and Procedure Review

Practical, well-written information security policies are key to managing an effective information security program. These policies define expectations and how to protect sensitive information. They guide behavior of your staff and form the basis of your organization's procedures and standards.

Our policy and procedure reviews are based on industry requirements such as GLBA, HIPAA/HITECH, PCI DSS, and general information security best practices, covering both technical and operational topics including:

- User access rights
- Acceptable use policies
- Network design and segmentation
- System configuration
- System patching and configuration management
- Secure application coding
- Physical and electronic access controls
- Event logging and review
- System security testing
- Firewall configuration
- Sensitive data minimization
- Sensitive data encryption
- Anti-virus systems
- Security log reviews
- Security information retention
- Incident response

Ongoing Support

Annual Support Agreement

An Annual Support Agreement is appropriate when you need guidance, ongoing support, and access to the Compliance Portal. Our team consults with yours when they have questions, provides guidance regarding the intent of compliance controls, and advice for remediating any flaws in your cybersecurity environment. This relationship starts from the moment you engage with CampusGuard and never ends as your environments and processes continue to evolve.

Whether you encounter an issue or need advice on addressing cybersecurity or compliance challenges, require consulting or technical support to answer questions or set direction, need assistance using the Compliance Portal, need to schedule additional assessments, or simply want to add training courses—you simply contact your dedicated Customer Advocate Team. Via regular newsletters and alerts, CampusGuard keeps you up to date on trends in cybersecurity, the latest news from regulatory agencies, and overall information about new threats that have been identified. Your dedicated CampusGuard Customer Advocate Team provides not only support during and after assessments but contributes toward your strategic cybersecurity goals year over year.

RFP Section V.B.2 and Section IV.A.5.e

Premier Partner Services

The Premier Partner Services program is appropriate when you may not have the available resources to provide the project management, remediation, and other necessary services to achieve your objectives. This comprehensive support offering includes a much more significant role for CampusGuard in assisting you to reach your specific cybersecurity and/or compliance goals. Since each initiative is unique, a series of discussions are held to understand the scope of work (SOW) and responsibilities of the parties. The service typically includes a combination of off-site and onsite support and project management for a specific period of time, with clear and understandable expectations for all parties. Once the SOW and agreement are completed and signed, the project commences, and a detailed project plan is developed that identifies the assignments and deliverable dates.

Expertise, Qualifications, and Experience

RFP Section V.B.3

CampusGuard was founded in 2009 and delivers professional services in the areas of IT security and compliance such as PCI DSS, FACTA/Red Flags, FERPA, HIPAA, GLBA, and other areas regarding the protection of sensitive information.

CampusGuard is certified by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) organization providing services in North America and Australia. Of approximately 390 QSA companies and 85 ASV firms certified by the PCI SSC, CampusGuard is the only company with the sole focus of providing PCI compliance products and services to multi-campus communities, such as higher education. We have unparalleled experience and focus on providing the very highest levels of PCI compliance services.

Our pattern of growth has remained positive over the last 13+ years, building upon customer success and not capital infusions from private investors or our parent company Nelnet, Inc. We have grown to employ a team of over 30 individuals who are strategically placed throughout the United States, working remotely to serve our customer base of over 400 state and local governments, healthcare organizations, and higher education institutions.

Our Security Advisors average more than 15 years' experience in information security and compliance, and our Customer Relationship team, comprised of responsive professionals, are dedicated to assisting your organization improve their overall information security posture with minimal impact to the business. Our employees possess the highest industry and technical certifications. All of our Security Advisors are CISSP, CISA, and QSA certified, and all of our CRMs have obtained their PCIP certification. This allows CampusGuard to guarantee that the individuals assigned to the University not only have the experience to provide excellent support, but they hold the credentials to back it up. The managerial team that will be involved in this relationship are outlined below.

Ed Ko, Director, Information Security Services

Ed has over 20 years' experience in providing information security and compliance services within campus-based environments. Prior to CampusGuard, Ed was an information technology and security analyst for The Pennsylvania State University. As a co-founder of CampusGuard, he has personally conducted and delivered hundreds of assessments, which have helped him ably lead our highly qualified and deeply experienced team of security professionals. Ed is well-respected in the information technology arena, possessing a well-rounded understanding of information technology and the issues it can resolve, all while maintaining a keen awareness of the unique challenges that are often associated with complex environments.

RFP Section V.B.3

Chad Wheeler, Manager, Offensive Security Services

Chad Wheeler has more than ten years of extensive experience in delivering offensive security services, evidenced by the extreme nature of penetration testing exercises he performed against the Department of Army Systems across the nation and against US Army websites. As Manager of CampusGuard's Offensive Security Services team, Chad is responsible for the team of professionals that provide penetration testing, vulnerability scanning, social engineering, and security assessments to our customers.

Chad has authored and restructured information assurance documentation, compliance reporting, and operating procedures during his time with the United States Army - leading the scanning, remediation, and hardening efforts for the infrastructure team during three Command Cyber Readiness Inspections and receiving "outstanding" scores for the Department of Army.

Judi Seguy, Director, Operations

Judi has over 30 years of experience working in fields related directly to information security and compliance, relationship management, project management, and more in higher education, government, and healthcare markets. Judi coordinates the timely and accurate delivery of information security and compliance services, defining all CampusGuard products and their associated implementation strategies, while at the same time developing internal tools to manage project scope, goals, and deliverables. In addition, Judi has direct responsibility for the overall development of training courses and customer communications.

As a member of the CampusGuard Leadership Team, Judi is the liaison between management and the Customer Advocate Teams. Along with various internal teams, Judi is able to define and implement processes for each service in order to ensure that every customer engagement achieves a consistent level of excellence.

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 13 Months 7

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
Virginia Tech	4/11-Present	Blacksburg, VA	Becky Ford 540.231.4543 & Joseph Goodman 540.231.6065
Christopher Newport U	4/10-Present	Newport News, VA	Peggy Taylor 757.594.8137 & Wendy Corrice 757.594.0704
Old Dominion U	5/13-Present	Norfolk, VA	Kate Rhodes 757.683.5403 & Branden Matthews 757.683.6274
Boar's Head Resort	3/16-Present	Charlottesville, VA	Dave Jefferson 434.972.6086
Virginia Military Institute	2/15-Present	Lexington, VA	Maj L. Vaughn 540.464.7725 & Col W. Robinson 540.464.7341
Radford U	2/11-Present	Radford, VA	William Shorter (540) 831-5794

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

   Main Office: 4740 N Cumberland Ave, Suite 365, Chicago, IL 60656

   Billing: 121 S. 13th Street, Suite 201, Lincoln, NE 68508

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: CampusGuard LLC **Preparer Name:** Jennifer Haack

Date: 10/10/22

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date: _____

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: RFP# FDC-1161 Date Form Completed: 10/10/22

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

Offeror / Proposer:

CampusGuard LLC (Firm) | 4740 N Cumberland Ave, Suite 365, Chicago, IL 60656 (Address) | Andrew Grant 419.873.7016 (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)
In general, CampusGuard does not utilize subcontractors of any kind. We provide all services in-house. However, we are wiling to assess opportunities to utilize SWaM subcontractors on a project-by-project basis.					

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

RETURN OF THIS PAGE IS REQUIRED

VASCUPP Member Sales

RFP Section V.B.6

The following figures are from the timeline of October 1, 2021 – September 30, 2022:

- Boar's Head Resort - $29,037.78
- Christopher Newport University - $13,088.33
- College of William and Mary - $15,436.47
- George Mason University - $18,061.47
- Longwood University - $26,573.63
- Norfolk State University - $0
- Old Dominion University - $24,692.78
- Radford University - $17,745.39
- University of Mary Washington - $45,622.27
- University of Virginia - $18,009.22
- University of Virginia Alumni Association - $14, 835.24
- University of Virginia Health - $25,096.28
- Virginia Commonwealth University - $999.00
- Virginia Military Institute - $17,816.47
- Virginia Tech - $20,581.96

Cost Proposal

RFP Section V.B.7

Cybersecurity and Compliance Assessments (NIST, HIPAA, PCI, GLBA, FERPA, etc.)	***Price***
1 Day - Remote	$9,900.00
2 Day - Remote	$12,900.00
3 Day - Remote	$14,900.00
4 Day - Remote	$16,900.00
5 Day - Remote	$18,900.00
1 Day - Onsite	$13,400.00
2 Day - Onsite	$17,300.00
3 Day - Onsite	$20,200.00
4 Day - Onsite	$23,000.00
5 Day - Onsite	$25,900.00
Report on Compliance Assessments	***Price***
3 Day PCI DSS Report on Compliance***	$44,950.00
4 Day PCI DSS Report on Compliance***	$49,950.00
5 Day PCI DSS Report on Compliance***	$54,950.00
****Applicable to PCI DSS ONLY. One onsite visit included in pricing for the period of days indicated.*	
Annual Support Agreements	***Price***
10 Hours**	$10,000.00
20 Hours**	$12,000.00
30 Hours**	$14,400.00
40 Hours**	$16,800.00
50 Hours**	$19,200.00
60 Hours**	$21,600.00
80 Hours**	$28,800.00
100 Hours**	$33,600.00
***Includes CampusGuard Central™ portal, PCI and HIPAA policy and procedure template library, quarterly external vulnerability scans, and hours for information security and compliance support.*	
Onsite Fee	***Price***
1 Day	$3,500
2 Days	$4,400
3 Days	$5,300
4 Days	$6,100
5 Days	$7,000
10 Days	*This will be handled as two 5-day trips*

- Note 1: The Onsite Fee includes travel time and travel and living expenses.
- Note 2: The Onsite Fee is assessed per visit.

RFP Section V.B.7

Off-Site Consulting Hours	***Price***
10 Hours	$3,000.00
20 Hours	$6,000.00
40 Hours	$12,000.00
60 Hours	$17,100.00
80 Hours	$22,800.00
100 Hours	$27,500.00
200 Hours	$55,000.00

CampusGuard Central ™ PCI Portal	***Price***
Includes electronic SAQs, Policy Templates, Secure Document Storage, Multiple Roles, unlimited MIDs	*Quoted per Customer*

Vulnerability Assessments & Penetration Testing (every test will be different and quoted for size and configuration based on estimated effort)	***Price***
Vulnerability Assessment (all types) - Hourly Rate	$255.00
Penetration Testing (all types) - Hourly Rate***	$255.00
License and Appliance annual fee for internal scans	$2,995.00
Social Engineering Campaigns - Hourly	$255.00
Physical Security Reviews - Hourly***	$255.00
****All services performed remotely. Requested travel and living expenses billed separately. Travel table included*	

Premier Partner Services	***Price***
Premier Partner Services	Quoted by project depending on scope

Online Training Courses	***Annual Price per Subscription***	
	VASCUPP Hosted	CampusGuard Hosted
Faculty / Staff	$6.00	$8.00
Students	$1.00	N/A

- Includes the following CampusGuard OLT Courses: Information Security Awareness, PCI DSS, GLBA, HIPAA, FERPA, FACTA/Red Flags, Phishing/Spear Phishing.
- Student pricing can only be used for educational curriculum. Student employees are considered equivalent to staff.
- Minimum purchase of 100 subscriptions per institution with supplemental increments in bundles of 50 subscriptions.
- Online training courses can be hosted by the institution on their own SCORM compatible LMS.
- CampusGuard reserves the right to audit subscription usage at each customer hosted environment every six months.
- CampusGuard hosted customers are subject to hosting fees of $2,400.00 per year per institution.

RFP Section V.B.7

Notes:

1. Prices in US Dollars and are valid for 120 days from the date of this proposal.
2. CampusGuard is able to provide our assessments in a remote or onsite capacity. Please note that our standard assessments are remote. Therefore, confirmation to an onsite presence will be confirmed and agreed to prior to travel arrangements being procured.
3. Assessment invoice will be issued upon completion of the remote assessment interviews or on-site services as a single invoice.
4. For the Annual Support Agreement (ASA), prices will be based on the term outlined in the Order Form signed by the customer, beginning on the 1st or 15th day of the month, closest to the Order Form execution date, and concluding after a period of 12 months.
5. A separate invoice will be generated for the ASA following the assessment interviews and prior to the start of the term.
6. Following the initial one 1-year term, the ASA annual fee will increase 5% per year after the first year.
7. Invoices for the ASA will be issued annually 45 days in advance of the renewal date.
8. Travel time for requested ASA Onsite Services will be applied as the actual round-trip travel time but will not exceed 12 hours per visit. Reasonable travel and living expenses for any requested Onsite Services will be billed separately or customer can choose to apply two hours of ASA time per day in lieu of travel and living expenses.
9. All penetration testing services will be accompanied by a Rules of Engagement (RoE) that will describe each penetration testing scope of work.
10. All penetration testing services will be performed remotely. Should onsite work be requested by customer, all travel time and reasonable travel and living expenses will be billed separately.
11. Invoices for penetration testing services will be issued upon delivery of the Penetration Test Report.
12. Penetration testing pricing may or may not include a re-test. Retest will be determined during the construction of the SOW.
13. OLT pricing includes unlimited access for enrolled staff/student up to the maximum number of subscriptions.
14. OLT will be delivered via SCORM files if hosted by customer.
15. The first five hours of content customization is delivered at $1500.00. Hours following the five hours can be completed at $300 per hour.
16. For CampusGuard hosted customers a onetime custom OLT branding can be completed at $995.00.
17. For CampusGuard hosted OLT customers a onetime single sign-on service can be completed at $2,195.00.
18. The parties both understand and acknowledge that any mutually agreed modification or addition of services or other terms must be on a written and executed Order Form. Any subsequently executed Order Form shall be subject to the terms of the Agreement, and any conflict between different Order Forms or an Order Form and Agreement shall be controlled by the later fully executed Order Form.

JAMES MADISON UNIVERSITY

Request for Proposal

RFP# FDC-1161

Higher Education Compliance Consulting Services

September 12, 2022

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

REQUEST FOR PROPOSAL
RFP# FDC-1161

Issue Date: **September 12, 2022**

Title: **Higher Education Compliance Consulting Services**

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

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

Sealed Proposals Will Be Received Until 2:00 PM on October 12, 2022 for Furnishing The Services Described Herein.

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

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

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

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature in Ink)

Name: _____
(Please Print)

Date: _____ Title: _____

Web Address: _____ Phone: _____

Email: _____ Fax #: _____

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

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

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

REQUEST FOR PROPOSAL

RFP # FDC-1161

TABLE OF CONTENTS

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals from qualified sources to enter into multiple contracts to provide Higher Education Compliance Consulting Services for James Madison University (JMU), an agency of the Commonwealth of Virginia. Initial contract(s) shall be for one (1) years with an option to renew for nine (9) 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 more than 3,000 faculty and staff. There are over 600 individual departments on campus that support seven academic divisions. The University offers over 120 majors, minors, and concentrations. Further information about the University may be found at the following website: http://www.jmu.edu.

The University currently uses a third-party vendor to provide Higher Education Compliance Consulting Services. Examples of compliance areas include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accessibility Act (HIPAA)
- Information Technology Compliance

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

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

IV. STATEMENT OF NEEDS

James Madison University desires to contract with a qualified firm(s) to provide expertise and a range of services to support the University's compliance with one or more higher education specific laws and regulations.

A. SPECIFIC SERVICES:

1. PCI DSS Consulting Services:

   a. Describe the firm's experience with the Payment Card Industry Data Security Standards and the administration of those standards within the higher education community.

   b. Describe the methodology used to maintain PCI compliance at a university.

   c. Describe the firm's role in the university's security program.

d. Describe the online system/interface the firm provides and how Self-Assessment Questionnaires (SAQ) are completed through the system.

e. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Describe the dedicated QSA/customer service team that would be assigned to the University.

f. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

2. GLBA Consulting Services:

a. Describe the firm's experience with the GLBA Safeguards within the higher education community.

b. Describe the methods and processes used to ascertain compliance at a university.

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

3. HIPAA Consulting Services:

a. Describe the firm's experience with HIPAA / HITECH compliance within the higher education community.

b. Describe the methods and processes used to ascertain compliance at a university.

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

4. FERPA Consulting Services:

a. Describe the firm's experience with FERPA within the higher education community.

b. Describe the methods and processes used to ascertain compliance at a university.

c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

5. IT Compliance Consulting Services:

    a. Describe the firm's experience with NIST 800-171 and ISO 27001 within the higher education community.

    b. Describe the methods and processes used to assist the university to adhere to the standards.

    c. Describe available training options and associated costs. Include a catalog of training offerings and differentiation between technical staff and end-user training.

    d. Provide the names, qualifications, and experience of personnel to be assigned to provide guidance and training to James Madison University. Designate who would be assigned as the primary contact for the university.

    e. Describe other technology-related consulting services available from your firm.

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

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

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

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

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

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

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

2. The version of the solicitation issued by JMU Procurement Services, as amended by an addendum, is the mandatory controlling version of the document. Any modification of, or additions to, the solicitation by the Offeror shall not modify the official version of the solicitation issued by JMU Procurement services unless accepted in writing by the

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

3. Proposal Preparation

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

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

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

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

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

   f. Ownership of all data, materials and documentation originated and prepared for the State pursuant to the RFP shall belong exclusively to the State and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by the offeror shall not be subject to public

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

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

B. SPECIFIC PROPOSAL INSTRUCTIONS

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

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

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

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

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

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

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

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

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

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

		Points
1.	Quality of products/services offered and suitability for intended purposes	30
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	15
		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 non responsive and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intra university mail system. It is the sole responsibility of the Offeror to ensure that its proposal reaches the issuing office by the designated date and hour.

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

F. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for a period of nine (9) successive one-year periods under the terms and conditions of the original contract except as stated in 1. and 2. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew shall be given approximately 90 days prior to the expiration date of each contract period.

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

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

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

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

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

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

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

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

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

1. It is the goal of the Commonwealth that 42% of its purchases are made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All

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

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

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

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

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

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

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

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

P. 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.

Q. 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.

R. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The Contractor assures that information and data obtained as to personal facts and circumstances related to students, faculty, and staff will be collected and held confidential, during and following the term of this agreement, and will not be divulged without the individual's and the agency's written consent and only in accordance with federal law or the Code of Virginia. Contractors who utilize, access, or store personally identifiable information as part of the performance of a contract are required to safeguard this information and immediately notify the agency of any breach or suspected breach in the security of such information. Contractors shall allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting. Contractors and their employees working on this project may be required to sign a confidentiality statement.

IX. METHOD OF PAYMENT

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

X. PRICING SCHEDULE

The Offeror shall provide an hourly rate for the proposed services. Hourly rates should include all billables (e.g. travel, lodging, etc.). Offeror may provide an offsite and onsite rate. Include pricing for all other products and services. The resulting contract will be cooperative and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2.

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

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

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

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

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

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

   Years_____ Months_____

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

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

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

ATTACHMENT B

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

Offeror Name: _____ Preparer Name: _____

Date: _____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date:_____

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

If yes, certification number: _____ Certification date: _____

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

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

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

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

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: _____ Date Form Completed:_____

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

Offeror / Proposer:

_____	_____	_____
Firm	Address	Contact Person/No.

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

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

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

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

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

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

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

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

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

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

ATTACHMENT D

Zone Map

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

List of member institutions by zones

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

JAMES MADISON UNIVERSITY

September 30, 2022

ADDENDUM NO.: One

TO ALL OFFERORS:

REFERENCE:	Request for Proposal No:	**RFP# FDC-1161**
	Dated:	September 12, 2022
	Commodity:	Higher Education Compliance Consulting Services
	RFP Closing On:	**October 12, 2022 2:00pm**

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

1. **Question: Is JMU seeking one vendor to provide all five services or is the goal of the RFP to create a pool of vendors to solicit proposals from for future projects?**

   Answer: JMU's preference is to contract with one firm who will provide all services for the University, for the duration of the contract.

2. **Question: Are vendors allowed to bid on select services? For example, would vendors be allowed to submit proposals for three out of the five services listed in Section IV. Statement of Needs?**

   Answer: Refer to Question 1 above.

3. **Question: Are there specific projects JMU has identified for each of the five service areas?**

   Answer: There is not a specific project. This will be the vendor that handles our routine QSA functions, such as, but not limited to: PCI training, compliance discussions, security review, etc.

4. **Question: For each of the service areas, is JMU seeking vendors to provide assessment services or education and training services or both?**

   Answer: Both.

5. **Question: To what extent are vendors expected to provide education and training services?**

   Answer: At a minimum, the selected vendor will "train-the-trainer" by keeping JMU's compliance specialist up to date on changes to PCI DSS. Other training will depend on the selected vendor. Describe the types of training that you offer.

6. **Question: For each of the service areas, what is the expected percentage or ratio of onsite versus remote work?**

   Answer: Routine campus visits are expected. One or two visits a year are expected – each typically lasting 2-2.5 days.

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

7. **Question: Who is the current third-party vendor that JMU uses for higher education compliance consulting services?**

   Answer: PCI and GLBA compliance are currently provided by CampusGuard.

8. **Question: Does the current third-party vendor that JMU works with provide services for all five areas listed in Section IV. Statement of Needs? If yes:**

   1. **How many projects were conducted through the previous contract?**
   2. **What is the total dollar value of the projects conducted through the previous contract?**

   Answer: Yes. JMU has consulted with the current vendor of HIPAA, FERPA, and other compliance questions in the past. CampusGuard provides consulting services for all of these areas and more.

   Sub-Answer 1: JMU had a fairly significant GLBA project with CampusGuard but most of the time JMU uses them to answer questions or consult on a particular issue.

   Sub-Answer 2: Previous years spend were between approximately 14k – 18k, annually.

9. **Question: Would vendors be allowed to submit proposals electronically in lieu of hard copy submissions?**

   Answer: No, electronic submissions are not acceptable for this RFP. However, proposers should include a digital copy of their proposal with their submission.

10. **Please clarify the level of participation desired for SWaM businesses. For each project conducted, is the use of a SWaM business a requirement or a goal? If it's a requirement, is there a specific percentage per project that must be allocated to a SWaM business?**

    Answer: The overall SWaM Goal of the Commonwealth is 42%. For specific categories JMU has goals of 3% Minority, 6% Woman, 3% Service Disable Veteran, 3% Micro with the remainder primarily going to the Small business category.

11. **We are required to complete and return a SWaM Utilization Plan (Attachment B of the RFP) as part of the proposal. If this is a convenience contract, we won't know what type(s) or services and the corresponding percentage of each project that can be subcontracted until we receive a specific Statement of Work from JMU. In Attachment B, is it acceptable for us to say that we will assess opportunities to utilize SWaM subcontractors on a project-by-project basis?**

    Answer: If your company cannot state specific sub-contractors or percentages, it is acceptable for your company to say that your company will assess opportunities to utilize SWaM subcontractors on a project-by-project basis.

12. **Question: Regarding the Small Business Subcontracting Plan, page 5 of the RFP states "This is a requirement for all prime contracts in excess of $100,000 unless no subcontracting opportunities exist." If this is a contract for as-needed services, individual contract holders may never exceed the $100,000 threshold. For this contract, what SWaM utilization expectations will the University have for each vendor's first $100,000 worth of contract activity?**

Answer: Our hope would be that regardless of the size of the needed service that a vendor would assess the opportunity to use SWaM certified sub-contractors as part of the project, and then report that usage to JMU on a quarterly or end of project basis.

13. **Question: End user training is referenced in a few sections. Please define the roles of the "end users" that will be trained for each category.**

    Answer: End users are the day-to-day users of the applicable section. For example, for PCI, we're referring to staff members who directly handle payment cards and review transactions.

14. **Question: Who is the complete audience for training?**

    Answer: Technical staff, business users, leadership, end users? We have staff at each of these levels and are interested in the training offered at all levels.

15. **Question: Is JMU seeking to train coworkers on PCI-DSS, GLBA, HIPAA, FERPA, and IT Compliance? If so, to what extent? To conduct assessments or just training on the various compliances?**

    Answer: Some of the compliance areas require regular (e.g. annual) training. Many of the areas require training as the regulations are updated. We are interested in learning what training offerings vendors provide.

16. **Question: What modality do you prefer for training – live, instructor-led, or self-paced?**

    Answer: JMU is interested in learning what trainings you offer. We have used all of these modalities in the past.

17. **Question: Can you please clarify if you would like experience performing a PCI QSA Assessment for a Level 1 Merchant? Or are you requesting experience about implementing a PCI program and maintaining PCI DSS compliance for a higher education entity?**

    Answer: JMU is a higher education entity with an existing PCI program.

18. **Question: Is this an opportunity to be JMU's PCI Advisory strategic partner? Or will the company be asked to help remediate known issues and maintain PCI DSS compliance? How long would the Company need to maintain JMU's PCI compliance?**

    Answer: JMU is seeking a qualified QSA firm to provide ongoing PCI support. That would include, but is not limited to, training, performing applicable security reviews, consulting for new services, on-site and remote process reviews, etc. JMU has an internal team that administers day-to-day decisions and activities. The length of the support would be based on the contract agreement.

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

Sincerely,
Doug Chester
Buyer Senior
Phone: 540-568-3137