REQUEST FOR PROPOSAL #92340
Managed Security Operations Center (SOC) Services

ISSUE DATE: October 21, 2026

SIGNIFICANT MILESTONES	DATE AND TIME
Pre-Proposal Conference	October 29, 2026, at 1:00pm – 2:00pm
Last Day for Questions	November 2, 2026, at 10:00 AM ET
Technical and Price Proposals Due	November 16, 2026, at 10:00 AM ET
Virtual Discussion Sessions	December 8 - 16, 2026 (anticipated)

NOTICE: Prospective Offerors who have received this document from a source other than the Issuing Office should immediately contact the Primary Procurement Officer and provide their name and email address in order to ensure that amendments to the Request for Proposal or other communications can be sent to them. Any Prospective Offeror who fails to provide the Issuing Office with this information assumes complete responsibility in the event that they do not receive communications from the Issuing Office prior to the closing date. It is the responsibility of the Prospective Offeror to monitor eMMA and Bid Locker for updates to advertised Solicitations.

University of Maryland Global Campus
3501 University Boulevard East
Adelphi, Maryland 20783
www.umgc.edu

eMaryland Marketplace Advantage (eMMA)
https://emma.maryland.gov/

Bid Locker
https://bidlocker.us/a/umgc/BidLocker

KEY INFORMATION SUMMARY SHEET

Request for Proposals	Security Operations Center (SOC) Services
Solicitation Number:	92340
Pre-Proposal Conference:	October 29, 2026, from 1:00 – 2:00PM (EST) via Microsoft Teams https://events.teams.microsoft.com/event/06740c87-a8a3-4930-866a-5fd2df11e055@704ce3d6-a4bf-4e09-8516-d52840c9f7a9?source=copyLinkLegacyShareEventDialog **This is a virtual meeting; no on-site conference will be held.**
Questions Due Date and Time:	November 2, 2026, at 10:00 AM ET
Technical and Price Proposal Due (Closing) Date and Time:	November 16, 2026, at 10:00 AM ET
MBE Subcontracting Goal:	An overall Minority Business Enterprise (MBE) subcontract participation goal of three percent (3%) of the total contract dollar amount, including all renewal option terms, if any, has been established for this procurement.
The dates below are for Shortlisted Offerors only	
Oral Presentations	December 8 – 16, 2026 (anticipated)
Contractor(s) Selection Anticipated	January 20, 2027 (anticipated)
Agreement Executed by Selected Contractor	March 1, 2027 (anticipated)
Agreement Executed by UMGC	After BPW Approval – UMGC will not go to BPW until after the awarded Contractor signs the Agreement

TABLE OF CONTENTS

KEY INFORMATION SUMMARY SHEET 2
TABLE OF CONTENTS 3
SECTION I. GENERAL INFORMATION 4
SECTION II. SCOPE OF WORK 11
ATTACHMENT A – UMGC CONTRACTOR STANDARDS 18
ATTACHMENT B – SERVICE LEVELS AND PERFORMANCE METRICS 20
SECTION III. PROCUREMENT PHASES AND EVALUATION PROCESS 23
ARTICLE 1. Information Required to be Submitted with the Technical Proposal 23
ARTICLE 2. TECHNICAL EVALUATION PROCESS 29
ARTICLE 3. PRICE PROPOSAL REQUIREMENTS 31
ARTICLE 4. FINAL EVALUATION, RANKING AND SELECTION 33
APPENDICES 34

SECTION I. GENERAL INFORMATION

1. Summary.

1.1. **Solicitation:** The intent of this Request for Proposals ("RFP" or "Solicitation") is to provide qualified vendors an opportunity to present their qualifications, experience, and conceptual approach to providing the scope of services in relation to the needs of the University of Maryland Global Campus ("the University" or "UMGC"). Proposals that concisely present the information requested in the order and manner requested will be considered more favorably than a Proposal ("Proposal" or "Offer") from an Offeror of commensurate qualifications that displays a lack of organization, conciseness, or attention to detail. Prospective bidders / offerors who obtained this document from the UMGC website, e-Maryland Marketplace, or any source other than the Procurement Officer(s), should provide their names and email addresses to the Issuing Office (see below) to ensure receipt of addenda and other communications regarding this solicitation.

1.2. **Procurement Regulations:** This RFP shall be conducted in accordance with USM Procurement Policies and Procedures. The procurement method is Competitive Sealed Proposals. The text of the Policies and Procedures is available at: http://www.usmd.edu/regents/bylaws/SectionVIII/VIII300.html.

1.3. **Background:** Go to http://www.umgc.edu/visitors/about/ for a profile of the University. We are proud to have had a global presence since 1949. While we offer online programs, we also offer more than 175 classroom and service locations worldwide, including many at military installations. Our locations span our Stateside location which can be accessed here: https://www.umgc.edu/locations. Our Europe locations, which can be accessed here: https://europe.umgc.edu/locations. And our Asia locations, which can be accessed here: https://asia.umgc.edu/locations. UMGC is known for our commitment to delivering a wide variety of respected online programs to working adults and military servicemembers, veterans, and their family members. We're also known for our reputation as a Maryland state university and our dedication to helping our students reach their academic and career goals. Read the UMGC Overview which can be access here: https://issuu.com/umucachiever/docs/umgc_overview_fy2025_a for an in-depth look at our culture of innovation and mission-driven service in action.

2. Issuing Office.

2.1. **Issuing Office:**

University of Maryland Global Campus
Office of Procurement Services
3501 University Blvd. East
Adelphi, MD 20783

Procurement Officers:

Alicia Klein
Director – Procurement
Alicia.klein@umgc.edu

Rosemary Williams
Senior Buyer - IT
rosemary.williams@umgc.edu

2.2. The Procurement Officer(s) shall be the point(s) of contact with the University for purposes of the preparation and submittal of proposals in response to this solicitation.

3. Questions and Inquiries.

3.1. All questions and inquiries regarding this procurement must be directed to the individual(s) referenced with the Issuing Office above. Inquiries will receive a written reply. Copies of replies will be sent to all other Offerors, but without identification of the inquirer. All such questions and inquiries must be received by the date and time as listed in the Key Information Summary Sheet above.

3.2. Offerors remain solely responsible for the content, accuracy, relevance, and appropriateness of all questions submitted. Questions generated through artificial intelligence (AI), automated tools, or other third-party technologies must be reviewed and validated by the Offeror prior to submission. UMGC requests that Offerors refrain from submitting generic, duplicative, speculative, or irrelevant questions that are not directly applicable to this solicitation. The submission of excessive, repetitive, or non-substantive questions may increase administrative burden and delay the procurement process for all participants. Offerors are expected to exercise professional judgment and conduct an appropriate review of the solicitation before submitting inquiries.

3.3. Questions that, in UMGC's reasonable discretion, appear to have been generated through AI without substantive review by the Offeror, may be omitted from UMGC's question and answer opportunities. This shall include, but not be limited to, questions already addressed within the solicitation. UMGC reserves the right to consolidate similar questions, decline to respond to questions deemed unrelated to the procurement, and determine whether a question warrants the issuance of an amendment or clarification.

4. Pre-Proposal Conference. If a Conference will be held, the date, time, and location is indicated on the Key Information Summary Sheet. Attendance at the Conference is not mandatory, but all interested parties are encouraged to attend in order to facilitate better preparation of their Proposals. Offerors shall submit their top three (3) questions in writing to the Procurement Officers prior to the pre-proposal conference. All potential Offerors should register using the link in the Key Information Summary Sheet. Attendees that do not submit a Please try to register at least 48 hours in advance. Appropriate auxiliary aids and services for qualified individuals with disabilities will be provided upon request. Contact the Procurement Officer(s) with specific requests at least five (5) business days prior to meeting.

MBE subcontractors are encouraged to attend the Conference to market their participation to potential prime contractors.

5. Proposal Closing Date/Due Date and Time.

5.1. **Technical Proposal:** Technical Proposals must be uploaded electronically at the UMGC Bid Locker link provided below no later than the date and time indicated in

the Solicitation Schedule. File names for the Technical Proposal documents are to include the RFP number and the Proposer's name. **NO PRICING INFORMATION** is to be provided in the Technical Proposal.

Bid Locker link for Technical Proposal upload:
https://bidlocker.us/details/6605_Rfp_92340___Managed_Security_Operations_Center_Soc_Services

Proposers must be registered on Bid Locker prior to uploading proposals. To register for a Bid Locker account, go to:

https://bidlocker.us/Account/Signup/UMGC.

Should you encounter any issues during account set-up or require additional assistance with Bid Locker, please reach out to Bid Locker directly at help@bidlocker.us or 267-225-1407. (*DO NOT wait until the due date for Proposals to sign up for an account; sign up as soon as possible.)

The University advises Proposers to allocate an adequate amount of time to create a Bid Locker account prior to any submission due date. It is also advisable to familiarize yourself with the Bid Locker site and the upload features and functionality related to uploading documents.

Proposers shall allow sufficient time in uploading the Technical Proposal to ensure timely receipt by the Issuing Office via the Bid Locker site. **Upon successful submission, Proposers may download a submission receipt on Bid Locker. Proposers will also receive an email confirmation within a few minutes from Bid Locker.** Proposers that do not receive confirmation should immediately notify the Issuing Office, and contact Bid Locker at help@bidlocker.us or 267-225-1407 to confirm that their Proposal has been received. **Proposers will not be able to upload Proposals after the due date and time, and late Proposals will not be considered.**

If any pricing information is included in the Technical Proposal, the Proposal may be deemed non-responsive by the Issuing Office. Hyperlinks to software products that indicate that the Technical Proposal is posted by the Proposer on an electronic site may be rejected or be considered non-responsive if a "Click-Through Agreement" is required to be accepted by UMGC in order to download the Technical Proposal.

By providing the Technical Proposal electronically to UMGC, the Proposer grants UMGC an unlimited right to generate additional electronic and/or paper copies for distribution solely for the purpose of evaluation and review.

5.2. **Price Proposal:** Price Proposals must be uploaded electronically at the UMGC Bid Locker link provided below no later than the date and time indicated in the Solicitation Schedule. File names for the documents are to include the RFP number and the Proposer's name.

Refer to Section III Article 3 for more information regarding Price Proposals.

Bid Locker link for Price Proposal upload:
https://bidlocker.us/details/6605_Rfp_92340___Managed_Security_Operations_Center_Soc_Services

5.3. Proposals should be provided in accordance with the Solicitation Schedule. Late Proposal submissions will not be accepted.

5.4. Neither Technical nor Price Proposals will be opened publicly. The identity of Offerors will not be disclosed prior to the Contract Award.

5.5. The Technical Proposal and/or Price Proposal, either individually or collectively, is considered by UMGC to be an Offer.

6. Minority Business Enterprises.

6.1. Minority participation is important to UMGC and the State of Maryland. State-certified Minority Business Enterprises (MBE) are strongly encouraged to respond to this solicitation notice and to attend the Pre-Proposal Conference. If not certified by the Maryland Department of Social and Economic Mobility (DOSEM), MBEs are encouraged to initiate certification as soon as possible. For more information on the State's MBE program or questions related to certification, please contact DOSEM's Office of Minority Business Enterprise/Equal Opportunity, telephone 800-544-6055 or view the DOSEM website: https://marylandmdbe.gob2g.com/?TN=marylandmdbe.

6.2. An MBE subcontracting goal of no less than three percent (3%) of the total overall contract value is established for this solicitation. Proposers are expected to meet or exceed this goal. This subcontracting goal will become part of the contract. It is imperative that awarded firms follow the MBE guidelines for subcontracting requirements. *If an MBE Prime Contractor is awarded the contract, this MBE subcontracting goal will still apply*.

6.3. Complete and sign the **MBE Utilization and Fair Solicitation Affidavit & MBE Participation Schedule Form** which can be accessed at this link: https://content.govdelivery.com/attachments/MDDGS/2026/09/01/file_attachments/3766548/Attachment%20D-1A%20-%20Effective%209-1-26%20-%20Compressed.pdf and include it with the Technical Proposal. This form is labeled as Attachment D-1A. The information on the form may not be submitted in another format.

PLEASE CONTACT THE UMGC MBE LIAISON, pamela.welzenbach@umgc.edu, IF YOU HAVE ANY QUESTIONS REGARDING COMPLETION OF THE ATTACHMENT D-1A PARTS 1, 2 AND 3 FORMS.

6.4. **Liquidated Damages Provision Related to MBE Goal**. The Contract resulting from this solicitation requires the Contractor to make good faith efforts to comply with the Minority Business Enterprise ("MBE") Program and Contract provisions. The State and the Contractor acknowledge and agree that the State will incur damages, including but not limited to loss of goodwill, detrimental impact on economic development, and

diversion of internal staff resources, if the Contractor does not make good faith efforts to comply with the requirements of the MBE Program and MBE contract provisions. The parties further acknowledge and agree that the damages the State might reasonably be anticipated to accrue as a result of such lack of compliance are difficult to ascertain with precision.

6.5. Therefore, upon a determination by the State that the Contractor failed to make good faith efforts to comply with one or more of the specified MBE Program requirements or contract provisions, the Contractor agrees to pay liquidated damages to the State at the rates set forth below. The Contractor expressly agrees that the State may withhold payment on any invoices as a set-off against liquidated damages owed. The Contractor further agrees that for each specified violation, the agreed upon liquidated damages are reasonably proximate to the loss the State is anticipated to incur as a result of such violation. Notwithstanding the use of liquidated damages, the State reserves the right to terminate the Contract and exercise all other rights and remedies provided in the contract or by law.

6.5.1. Failure to submit each monthly payment report in full compliance with COMAR 21.11.03.13B(3): $25.00 per day until the monthly report is submitted as required.

6.5.2. Failure to include in its agreements with MBE subcontractors a provision requiring submission of payment reports in full compliance with COMAR 21.11.03.13B(4): $100 per MBE subcontractor.

6.5.3. Failure to comply with COMAR 21.11.03.12 in terminating, canceling, or changing the scope of work/value of a contract with an MBE subcontractor and/or amendment of the MBE participation schedule: the difference between the dollar value of the MBE participation commitment on the MBE participation schedule for that specific MBE firm and the dollar value of the work performed by that MBE firm for the contract.

6.5.4. Failure to meet the Contractor's total MBE participation goal and the subgoal commitments: the difference between the dollar value of the total MBE participation commitment on the MBE participation schedule and the MBE participation actually achieved.

6.5.5. Failure to promptly pay all undisputed amounts to an MBE subcontractor in full compliance with the prompt payment provisions of this contract: $100 per day until the undisputed amount due to the MBE subcontractor is paid.

7. **Signing of Forms.** A Proposal, if submitted by an individual, shall be signed by the individual. If submitted by a partnership, a Proposal shall be signed by such member(s) of the partnership with authority to bind the partnership. If submitted by a corporation, a Proposal shall be signed by an officer and attested by the corporate secretary or an assistant corporate secretary; if not signed by an officer, there must be attached a copy of a board resolution or that portion of the by-laws, duly certified by the corporate secretary, showing the authority of the person so signing on behalf of the corporation.

8. **Acceptance of Terms and Conditions.** By submitting a Proposal, an Offeror shall be deemed to have accepted the terms, conditions, and requirements set forth

in this RFP. The RFP including all addenda in total shall be incorporated into the Contract by reference.

9. Contractual Agreement and Term.

9.1. The University intends to award one (1) contract with a single, qualified Offeror as a result of this Solicitation.

9.2. The contract to be entered into as a result of this RFP shall be by and between the Offeror as Vendor/Contractor and UMGC in the form of a University Contract and shall contain the mandatory provisions included in Appendix C as well as any additional terms required by UMGC or the State of Maryland. Exceptions, if any, must be clearly identified in the transmittal letter enclosed with the technical proposal. As deemed in the best interest of the University, mutually agreeable modifications of the solicitation provisions, if allowed by law, will be documented by express identification in the final contract as superseding the pertinent provisions of the solicitation.

9.3. The initial term of any contract arising from this RFP action shall commence on the date the contract is executed on behalf of UMGC, or such other date as UMGC and the Contractor shall agree. It is anticipated that the award will be subject to the approval of the State of Maryland Board of Public Works and may be subject to the approval of the USM Board of Regents. Upon receipt of all required approvals, the University will execute the Contract with the awarded Contractor.

9.4. The contract shall be in effect for an initial term of three (3) years, unless otherwise extended, expired, or terminated pursuant to the Contract. There are two (2), one-year renewal options at UMGC's sole option.

9.5. Maximum Contract Value: The aggregate value of all Services provided under the Contract shall not exceed the amount approved by the USM Board of Regents and/or Maryland Board of Public Works.

10. Confidentiality of Offeror's Information. Refer to Appendix S for the terms of confidentiality of UMGC's and Offeror's information.

11. Post-Award Confidentiality. Refer to Appendix C-1 for the confidentiality obligations of awardee and UMGC.

12. Insurance Requirements. The Contractor must maintain, at a minimum, the insurance coverages outlined below, or any minimum requirements established by law if higher, for the duration of the Contract, including option periods, if exercised. The following type(s) of insurance and minimum amount(s) of coverage are required:

12.1. Commercial General Liability - One million dollars ($1,000,000) combined single limit per occurrence for bodily injury, property damage, and personal and advertising injury and three million dollars ($3,000,000) annual aggregate. The minimum limits required herein may be satisfied through any combination of primary and umbrella/excess liability policies.

12.2. Cyber Security/Data Breach Insurance – Five million dollars ($5,000,000) per occurrence. The coverage must be valid at all locations where work is performed or

data or other information concerning the University's claimants or employers is processed or stored.

12.3. Worker's Compensation - The Contractor shall maintain such insurance as necessary or as required under Workers' Compensation Acts, the Longshore and Harbor Workers' Compensation Act, and the Federal Employers' Liability Act, to not be less than one million dollars ($1,000,000) per occurrence (unless a state's law requires a greater amount of coverage). Coverage must be valid in all states where work is performed.

(End Section I. General Information)

SECTION II. SCOPE OF WORK

1. **Purpose.** This Scope of Work defines the scope, responsibilities, deliverables, service levels, and operational requirements for the provision of Managed Security Operations Center (SOC) services by a Managed Security Services Provider (MSSP) for the University of Maryland Global Campus (UMGC). Go to http://www.umgc.edu/visitors/about/ for a profile of the University. We are proud to have had a global presence since 1949. While we offer online programs, we also offer more than 175 classroom and service locations worldwide, including many at military installations. Our locations span our Stateside location which can be accessed here: https://www.umgc.edu/locations. Our Europe locations, which can be accessed here: https://europe.umgc.edu/locations. And our Asia locations, which can be accessed here: https://asia.umgc.edu/locations. UMGC is known for our commitment to delivering a wide variety of respected online programs to working adults and military servicemembers, veterans, and their family members. We're also known for our reputation as a Maryland state university and our dedication to helping our students reach their academic and career goals. Read the UMGC Overview which can be accessed here: https://issuu.com/umucachiever/docs/umgc_overview_fy2025_a for an in-depth look at our culture of innovation and mission-driven service in action.

   The term “Contractor” or “MSSP” used throughout the scope of work refers to the awarded firm. The term “Contract” used throughout the scope of work refers to the anticipated contract issued to the awarded firm.

   The MSSP will support and advance the maturity of the University's cybersecurity operations through continuous security monitoring, threat detection and analysis, incident response support, reporting, and strategic security advisory services. These services are intended to enhance UMGC's operational security capabilities while maximizing the value of existing security technologies and investments within the University's environment.

   Through this engagement, the MSSP will help reduce cyber risk, strengthen the protection of sensitive institutional data, and support compliance with applicable higher education regulatory and security requirements.

   These services aim to reduce cyber risk, protect sensitive student, faculty, research, and administrative data while supporting compliance with higher regulatory obligations such as University System of Maryland (USM) IT Security Standards, NIST Cybersecurity Framework (CSF), NIST SP 800-171, FERPA, GLBA, PCI DSS, CMMC, and NIST frameworks.

   The Contract requires one (1) designated Key Personnel position: Service Operations Manager. The proposed Service Operations Manager may be based within the United States or at a nearshore location. Nearshore means a location outside the United States that is located within the Western Hemisphere and operates in a time zone that substantially overlaps with U.S. Eastern Time business hours.

2. **Current State.** The threat landscape is evolving at a rapid rate with the advent of Artificial Intelligence (AI). Bad actors are now capable of creating malicious packages and brute-force login attempts targeting employee and student accounts at a much higher rate than previously seen. In the last quarter, the number of security alerts in our Microsoft environments doubled. A delay in the identification of and response to an incident could

potentially increase the impact above acceptable levels. As the vulnerability and threat landscape evolves, The University has identified the need to augment current security operations tasks to enhance the ability to identify, triage, and address potential incidents in an accelerated fashion.

Currently, cybersecurity incident response at UMGC is managed by the Security Operations team, which is responsible for a broad range of operational and strategic initiatives, including security monitoring, alert triage, incident investigation, and response activities. As part of its ongoing cybersecurity program development, UMGC is actively maturing its incident response capabilities to enhance the organization's ability to detect, analyze, and respond to security incidents in a timely and effective manner.

Key initiatives supporting this effort include expanding Security Information and Event Management (SIEM) coverage, developing and refining detection policies and use cases, creating and maintaining incident response playbooks, and implementing automation to improve operational efficiency and consistency. These efforts are focused on reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) while ensuring that incidents are managed, documented, and resolved in accordance with established processes and best practices.

To further strengthen its security posture, UMGC requires a managed Security Operations Center (SOC) capability that delivers specialized cybersecurity expertise and continuous 24x7 monitoring and response services. The SOC provides support and execution of incident response and management and will escalate issues to UMGC for awareness and decision making. This approach enables UMGC to maintain comprehensive security operations coverage while avoiding the significant staffing and operational costs associated with building and maintaining a fully internal SOC.

3. Scope of Services.

3.1. **Security Operation Services (SOC).** The MSSP will deliver end-to-end SOC services including:

- 3.1.1. 24x7x365 monitoring and analysis of security events using the University’s approved security monitoring platforms and telemetry sources.
- 3.1.2. cybersecurity incident detection, triage, escalation, containment, and response coordination.
- 3.1.3. improvement of the maturity, consistency, and execution of the University's incident response program.
- 3.1.4. optimization and definition of use cases and policies within the existing SIEM platform.
- 3.1.5. services that integrate with the University's current security ecosystem, minimizing disruption and maximizing operational efficiency.
- 3.1.6. delivery of actionable security reporting, metrics, and insights aligned with the University's risk management objectives, compliance requirements, and operational decision-making needs.
- 3.1.7. a Service Operations Manager as the primary point of contact and operational escalation point. This role is considered Key Personnel as defined in the Contract in Appendix C.
- 3.1.8. clearly defined reporting structures, documented roles and responsibilities, and performance expectations for all assigned personnel.

3.2. **As-Needed Services and One-Time Projects.** The University may, at its sole discretion, request additional cybersecurity services beyond the routine managed SOC services described above. The Contractor may make qualified cybersecurity personnel available to perform such services upon request and subject to mutually agreed work assignments. The University does not guarantee any minimum utilization of services under this section. Work performed under this section shall be authorized by the University and compensated in accordance with the rates established under the Contract. Unless otherwise authorized in writing by the University, work performed under this section shall be conducted on a time-and-materials basis using the rates established in the Contract.

4. Service Expectations. This section describes the detailed activities expected as part of the routine SOC services:

4.1. **Security Monitoring & Detection.**

4.1.1. Continuous monitoring and analysis of security events, logs, and telemetry generated across the University's SIEM tool.

4.1.2. The identification, triage, and analysis of potential security incidents, while minimizing false positives.

4.1.3. Correlation and analysis of security events across academic, administrative, cloud, and enterprise systems to identify suspicious activity and emerging threats.

4.1.4. Development, tuning, and maintenance of detection use cases, analytics, and alerting rules to improve detection effectiveness and align with the evolving higher education threat landscape.

4.1.5. Escalation of validated incidents in accordance with approved incident response procedures and service level requirements.

4.1.6. Annual review and update of SOC Operations Runbook, including incident handling procedures, notification requirements, and escalation workflows.

4.1.7. Maintenance of Incident Severity and Escalation Matrix defining roles, notification timelines, and escalation criteria.

4.1.8. Documentation updates reflecting operational, process, and technology changes.

4.2. **Incident Response Process Maturation.**

4.2.1. Review and enhancement of incident response procedures, escalation matrix, and response playbooks.

4.2.2. Development and refinement of incident classification criteria, prioritization methodologies, and severity definitions tailored to academic environments.

4.2.3. Implementation and optimization of automated detection, investigation, and response capabilities within SIEM.

4.2.4. Recommendations and process improvements designed to reduce Mean Time to Detect (MTTD), Mean Time to Acknowledge (MTTA), and Mean Time to Respond (MTTR).

4.2.5. Facilitation of quarterly incident response tabletop exercises and after-action reviews with the UMGC Security Operations (SecOps).

4.2.6. Alignment of policies and procedures with applicable industry standards and recognized cybersecurity frameworks, such as NIST 800-61r2.

4.2.7. Annual review and update of Incident Response Plan, including recommendations for process improvements and alignment with applicable cybersecurity frameworks and University requirements.

4.2.8. Maintenance and enhancement of Incident Response Playbooks for common security event and incident scenarios.

4.2.9. Documentation of automation workflows and operational procedures, where applicable.

4.3. **Tooling & Integration.**

4.3.1. Utilization of approved security platforms, including SIEM, Endpoint Detection and Response (EDR), Intrusion Detection/Prevention Systems (IDS/IPS), Data Loss Prevention (DLP), Network and Perimeter Security, vulnerability management tools, and related security technologies. Specific platforms will be shared with the awarded Contractor.

4.3.2. Support for onboarding and integration of new log sources, systems, and applications to improve security visibility and monitoring coverage.

4.3.3. Identification and implementation of tuning recommendations to improve detection quality, reduce alert fatigue, and increase operational efficiency.

4.3.4. Maintenance of baselines and runbooks.

4.3.5. Recommendations for enhancements to security telemetry, monitoring coverage, and tool utilization.

4.3.6. Maintain existing UMGC SIEM Detection Catalog, including approved use cases and alert logic.

4.3.7. Documentation of newly developed or enhanced detection rules, correlation logic, and monitoring coverage improvements.

4.3.8. Quarterly recommendations for tuning and optimization of security monitoring capabilities.

4.4. **Threat Intelligence & Proactive Defense.**

4.4.1. Integration of threat intelligence, relevant to higher education (e.g., ransomware, financial aid, research theft) into monitoring, detection, and investigation activities.

4.4.2. Analysis and contextualization of threats impacting higher education institutions, including threats targeting academic operations, research environments, financial systems, and user accounts.

4.4.3. Proactive threat hunting activities based on indicators of compromise (IOCs), threat actor tactics, techniques, and procedures (TTPs), and observed attack trends, relevant to higher education institutions.

4.4.4. Recommendations to strengthen the University's security posture based on identified threats, vulnerabilities, and operational observations.

4.5. **Reporting & Metrics.** Expected reporting, cadence, and contents (at a minimum) are listed below:

Cadence/Report Name	**Contents (at a minimum)**
Operational Reporting Dashboard – Real-time operational dashboard available for UMGC personnel to view daily.	Summary of security monitoring activities. Security investigations and incident activity. Notable threats, vulnerabilities, and observed trends. Open incidents and ongoing response activities.
Monthly Service Report	Security event and alert volumes. Incident volumes, categories, and trends. Mean Time to Detect (MTTD) and other agreed-upon service metrics (see Attachment B).

	Service-level performance results. False positive rates and detection tuning activities. Incident escalation performance. Key operational activities completed during the reporting period. Recommendations for service improvements and operational enhancements.
Quarterly Executive Report	Trend analysis and significant observations. Security risk themes and threat landscape updates. Root cause and incident trend analysis. Service-level performance and KPI summaries. Significant accomplishments and operational improvements. Strategic recommendations for enhancing detection, response, governance, and overall security operations maturity.
Quarterly Threat Intelligence Report	Highlight emerging threats, vulnerabilities, adversary tactics, and trends relevant to higher education institutions.
Major Incident Report (report as occurs)	Incident timelines, actions taken, findings, containment activities, remediation efforts, and resolution outcomes.
Post-Incident Report (report as occurs)	Lessons-learned and recommendations for significant security incidents, including opportunities for process, technology, and operational improvements.

4.6. **Governance & Communication.**

4.6.1. Participation in weekly operational meetings and quarterly strategic reporting.

4.6.2. Alignment of service delivery with applicable University policies, contractual requirements, and relevant cybersecurity and regulatory frameworks, including NIST Cybersecurity Framework (CSF), NIST SP 800-171, FERPA, and GLBA, as applicable.

4.6.3. Maintenance of documented communication and escalation procedures.

4.6.4. Timely escalation and notification of security incidents in accordance with approved severity matrix and service level requirements.

4.7. **MSSP Responsibilities.** The MSSP shall be responsible for delivering the services defined in this Statement of Work, including the operation and management of agreed-upon security monitoring, threat detection, incident response support, reporting, and advisory services. The MSSP shall provide qualified personnel, maintain effective communication with UMGC stakeholders, and perform all services in accordance with

established service levels, governance requirements, and documented operational procedures.

4.8. **UMGC Responsibilities.** UMGC shall provide the MSSP with the access, information, and resources reasonably required to perform the services outlined in this Statement of Work. UMGC shall maintain ownership of its systems, security tools, and data; provide timely decisions and approvals; and engage appropriate stakeholders to support incident response, remediation activities, governance processes, and service reviews.

4.9. **Shared Responsibilities.** UMGC and the MSSP shall collaborate to maintain effective security operations through regular communication, coordinated incident management, continuous service improvement, and periodic review of operational procedures, performance metrics, and security objectives.

5. Transition (Contract End). The Contractor shall be responsible for ensuring a seamless transition of services at the conclusion of the Contract. At a minimum, the Contractor's transition responsibilities shall include:

5.1. Develop and Submit a Transition-Out Plan. Submit a comprehensive plan for transferring services and knowledge to UMGC and/or the incoming provider. Upon contract conclusion, it is not anticipated that the Contractor will need to return any UMGC data or assets, as UMGC data remains within UMGC's systems and physical assets such as computers, monitors, and headsets belong to the Contractor however; the Contractor will certify in writing that no Contractor personnel retain access or confidential information upon contract termination. The Contractor must ensure all access is securely disabled as directed by UMGC.

5.2. Knowledge and Documentation Transfer. Facilitate knowledge transfer sessions, provide all relevant documentation, and respond to questions from UMGC and/or the incoming provider. Handover all Contractor-created documentation, reports, or training materials relevant to ongoing operations.

5.3. Access Termination. UMGC will initiate and execute the technical removal or disabling of user accounts, credentials, and permissions in UMGC systems. Contractor is responsible for: providing a complete list of all personnel (and any third parties) who have been given access to UMGC systems, confirming that all credentials are disabled, acknowledging in writing that their staff no longer require access and have not retained any confidential information, and assist UMGC by promptly reporting any issues or anomalies during the access termination process.

5.4. Availability of Key Personnel. Ensure Key Personnel are available for a defined transition period not to exceed thirty (30) business days after Contract conclusion to support handover activities.

5.5. Final Transition Reporting. Submit a final report summarizing all transition activities, outstanding issues, and recommendations for ongoing service delivery.

6. Implementation Success Criteria. The implementation phase shall be considered complete when the Contractor:

6.1. Completes all onboarding activities identified in the approved project plan;
6.2. Successfully integrates and validates all agreed-upon monitoring, logging, escalation, and communication capabilities;
6.3. Provides all required onboarding-related documentation and artifacts;
6.4. Demonstrates operational readiness to deliver the Services in accordance with this Statement of Work.

7. Minimum Qualifications: To be reasonably susceptible of being selected for award, an Offeror must meet the following minimum qualifications as of the Technical Proposal due date. Experience of subcontractors, affiliates, parent companies, technology partners, or other third parties will not be considered when determining whether the Offeror satisfies minimum qualification requirements. Failure to demonstrate compliance with the minimum qualifications may result in the Technical Proposal being determined not reasonably susceptible for award.

7.1. The Offeror must have a current ISO/IEC 27001 certification issued by an accredited certification body OR a current SOC 2 Type II attestation applicable to the services proposed under this solicitation. The Offeror must submit documentation as further described in Section III. Article 1, demonstrating compliance with this requirement.

7.2. The Offeror must submit the required references, as further described in Section III. Article 1.

7.3. The Offeror must submit the required case studies. as further described in Section III. Article 1.

8. Attachments. The following attachments are incorporated into and form a part of this solicitation. Offerors should review the attachments and provide any required information identified in the Technical Proposal Requirements section.

8.1. Attachment A – UMGC Contractor Standards. This attachment communicates UMGC's required and preferred standards applicable to the proposed solution and services.

8.2. Attachment B – Service Level Expectations. This attachment identifies UMGC's required and preferred service-level expectations.

(*balance of page left intentionally blank)*

ATTACHMENT A – UMGC CONTRACTOR STANDARDS

1. Performance Standards. The Contractor shall ensure continuity of services through appropriate resource planning, knowledge transfer, document maintenance, and transition support when personnel changes occur. Any staffing transitions (excluding Key Personnel) shall be managed in a manner that minimizes operational disruption and preserves institutional knowledge. Following transition to steady-state operations, Contractor performance shall be evaluated based on compliance with the Service Levels, Operational Performance Metrics, reporting requirements, and other obligations set forth in the Contract.

2. Project Management Standards. UMGC utilizes Microsoft 365 tools, including SharePoint, for project documentation and collaboration, and primarily uses Smartsheet for project management and reporting. The Contractor shall work within UMGC's Smartsheet environment (if applicable).

3. Artificial Intelligence ("AI") Preferred Standards. UMGC prefers solutions that utilize AI in a responsible, transparent, and educationally appropriate manner.

3.1. AI capabilities should support the delivery of reliable, accurate, and instructionally appropriate outputs that align with defined learning objectives, skills frameworks, competencies, and program outcomes. AI-enabled functions should minimize material errors and provide outputs that are relevant to the learner's context and intended use.
3.2. Where AI is used in content development, maintenance, or updates, the solution should ensure that appropriate controls and review processes are in place to maintain quality, accuracy, alignment, and accessibility. UMGC prefers solutions that incorporate human oversight and validation of AI-generated or AI-assisted content and that maintain alignment with accessibility, instructional, and quality standards throughout the content lifecycle.
3.3. AI capabilities should operate in a manner that is predictable, explainable at a functional level, and appropriate for use in an educational environment.

4. Security & Compliance Requirements. Contractor shall:

4.1. Maintain compliance with all applicable institutional policies and regulatory requirements, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and other relevant industry or legal obligations applicable to UMGC's environment.

4.2. Conduct all security monitoring, incident response, threat detection, and related SOC activities in alignment with recognized cybersecurity frameworks and guidance, including the NIST Cybersecurity Framework (CSF), NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations), and NIST Special Publication 800-61 (Computer Security Incident Handling Guide).

4.3. Implement and maintain secure communications, access controls, and administrative processes designed to protect UMGC systems and data. Access to UMGC environments shall be granted on the least privilege basis and limited to authorized Contractor personnel with a documented business need.

4.4. Establish and maintain appropriate safeguards to ensure the confidentiality, integrity, and availability of UMGC information and systems throughout the duration of the engagement.

4.5. Promptly notify UMGC of any security events, incidents, or compliance concerns that may impact UMGC systems, data, or regulatory obligations, in accordance with established escalation procedures and service level requirements.

(*balance of page left intentionally blank)*

ATTACHMENT B – SERVICE LEVELS AND PERFORMANCE METRICS

1. Incident Priority Definitions.

1.1. "Critical Severity" or "Sev 1" shall mean an active compromise of critical systems, widespread impact, regulatory risk, and/or business outage. Example incidents: Ransomware outbreak, domain admin compromise, active data exfiltration, breach of production environment.

1.2. "High Severity" or "Sev 2" shall mean a confirmed malicious activity affecting important systems but contained. Example incidents: Privileged account compromise, malware on production server, critical vulnerability being actively exploited.

1.3. "Medium Severity" or "Sev 3" shall mean a suspicious activity requiring investigation, limited business impact. Example incidents: Repeated failed login attempts, phishing clicks without compromise, malware quarantined by EDR.

1.4. "Low Severity" or "Sev 4" shall mean informational events or low-risk anomalies. Example incidents: Single failed login, vulnerability scan detection, policy violations.

1.5. "Informational" or "Sev 5" shall mean an event with no immediate risk. Example incidents: system alerts, routine monitoring, notifications, audit events.

2. Incident Response Times and Escalation Expectations. UMGC's desired incident response times and escalation expectations are as follows.

For purposes of this section "Mean Time to Detect (MTTD)" means the time elapsed between the occurrence of a security event and its detection by the SOC.; "Mean Time to Respond (MTTR)" means time required to initiate response and containment activities following the identification of a security incident.

Severity Level	**Mean Time to Detect (MTTD)**	**Mean Time to Respond (MTTR)**	**Escalation**
Critical	Fifteen (15) minutes	Fifteen (15) minutes	Immediate executive and incident response escalation
High	Thirty (30) minutes	One (1) hour	SOC Manager, Security Lead, IT Operations
Medium	One (1) hour	Four (4) hours	Security Operations Team
Low	Four (4) hours	One (1) business day	Ticket creation only
Informational	Next business day	Not applicable	Logging/reporting only

3. Operational Performance Metrics.

Metric	**Target**	**Definition**

Mean Time to Detect (MTTD)	≤ 90%	Percentage of security incidents detected within the MTTD response per severity level
Mean Time to Respond (MTTR)	≤ 90%	Percentage of security incidents detected within the MTTR response time per severity level
False Positive Rate	< 10%	Percentage of alerts investigated and determined not to represent a legitimate security threat or incident.
Reporting Timeliness	100%	Percentage of required operational, incident, management, and executive reports within agreed-upon reporting timeframes.
Incident Escalation	100%	Percentage of Severity Critical and Severity High incidents escalated to designated UMGC personnel in accordance with established escalation procedures and notification requirements

4. **Performance Measurement.** Performance against the Incident Response Times and Operational Performance Metrics defined herein shall be measured monthly and documented in Contractor's Monthly Service Report.

5. **Service Credits.** UMGC expects the Contractor to meet or exceed the Service Levels identified herein. Offerors are encouraged to propose an appropriate service credit methodology associated with failure to achieve the Service Levels identified herein. UMGC's preference is that any earned service credits will be applied to the Contractor's next monthly invoice. An example of the kind of methodology is provided below:

MTTD Performance

Monthly Achievement Rate	Service Credit
90% or greater	No Credit
85% - 89.99%	2%
80% - 84.99%	5%
Less than 80%	10%

MTTR Performance

Monthly Achievement Rate	Service Credit

90% or greater	No Credit
85% - 89.99%	2%
80% - 84.99%	5%
Less than 80%	10%

5.1. The total service credits assessed during any reporting month shall not exceed fifteen percent (15%) of the applicable monthly service fee.

5.2. If the Contractor fails to achieve any Critical Service Level during two (2) consecutive reporting months, or three (3) reporting months within any rolling six-month period, the Contractor shall submit a written corrective action plan to the University within ten (10) business days.

5.3. The corrective action plan shall identify the root cause of the service-level failure, actions to be taken to prevent recurrence, responsible parties, and implementation timelines.

5.4. Failure to achieve any Critical Service Level during three (3) consecutive reporting months, or four (4) reporting months within any rolling twelve-month period, may be considered a material breach of the Contract and may give rise to the University's rights and remedies under the Contract, including termination for cause.

(End Section II. Scope of Work)

(*balance of page left intentionally blank)*

SECTION III. PROCUREMENT PHASES AND EVALUATION PROCESS

ARTICLE 1. Information Required to be Submitted with the Technical Proposal

A. General Requirements.

A.1. The Offeror shall submit a complete Technical Proposal containing all information, forms, certifications, and supporting documentation required by this solicitation. Required forms and the Transmittal Letter may be uploaded as separate attachments. There is no limit on how many files you can upload, but right now, each file must be less than 1.5gb in size. Failure to comply with the requirements of this Article 1 may result in the technical proposal being deemed non-responsive. UMGC does not seek general descriptions of an Offeror's products, services, or capabilities. The Technical Proposal must directly address the requirements of this RFP. Generic marketing materials, product brochures, boilerplate content, standard sales presentations, and other promotional information may be provided as separate attachments, not within the body of the Technical Proposal.

A.2. Proposals must be paginated and prepared in a clear and concise manner that addresses each part of the RFP. **Price information shall not be included in the Technical Proposal.**

B. Transmittal Letter. Offeror shall include a transmittal letter/executive summary that clearly and concisely summarizes the content of the Technical Proposal. The transmittal letter must be signed by an individual who is authorized to bind the firm to all statements, including services and financial statements, contained in the Technical Proposal. Include the Offeror's official business address. **Price information shall not be included in the transmittal letter or elsewhere in the Technical Proposal.**

C. Offeror Qualification: Information Security Certification. Offerors shall complete the Offeror Qualification: Information Security Certification form in Appendix A, and provide the supporting documentation identified therein.

D. Technical Proposal Contents. Offeror shall address each item below, confirming compliance and describing in succinct detail how Offeror proposes to meet or exceed UMGC's objectives.

D.1. **Company Experience.** Offerors shall provide one (1) to three (3) case studies illustrating the Offeror's ability to deliver services comparable to those requested by UMGC. At least one (1) case study must include a new SOC implementation. Each case study should be two (2) pages or less. For each case study, provide:

D.1.1.1. Client name (if disclosure is permitted) or industry/sector (e.g. higher education, government, healthcare, financial services, etc.);

D.1.1.2. Scope of services provided;

D.1.1.3. Indicate whether the engagement included a new SOC implementation;

D.1.1.4. Duration of the engagement;

D.1.1.5. Client environment characteristics, including approximate number of users, endpoints, monitored assets, geographic distribution, and other factors relevant to the scope and complexity of the engagement;

D.1.1.6. Measurable outcomes achieved, such as improvements in detection capabilities, incident response performance, security visibility, threat reduction, compliance objectives, operational efficiencies, or other relevant metrics;

D.1.1.7. Information regarding applicable regulatory, security, or compliance frameworks supported by the engagement (e.g., NIST CSF, NIST SP 800-171, FERPA, GLBA, PCI DSS, CMMC).

D.1.1.8. Identify whether the services were delivered directly by the Offeror or through subcontractors, technology partners, managed service providers, or other third parties, and describe the Offeror's role in the engagement.

D.2. **SOC Operating Model.** Describe the proposed Security Operations Center (SOC) operating model and approach for delivering the services described in the Scope of Work. Clearly distinguish between services performed by the Offeror and services performed by any subcontractors, technology partners, managed service providers, or other third parties. Identify:

D.2.1. The entity or entities that own and operate the SOC providing the proposed services.

D.2.2. The location(s) from which SOC services will be delivered, including any domestic, offshore, or follow-the-sun operations.

D.2.3. The staffing and coverage model, including analyst coverage by shift, hours of operation, weekend and holiday coverage, and procedures for reviewing and escalating security events outside of normal business hours;

D.2.4. All subcontractors, technology partners, managed service providers, and other third parties involved in delivering the proposed services. Clearly describe the responsibilities of each entity;

D.2.5. The governance and service delivery model, including how the Offeror coordinates activities among all parties involved in providing the services.

D.2.6. In addition, Offeror must include the following table indicating the source of the performance for each function (ex: Offeror, subcontractor, etc.):

Function	Who Will Perform? (ex. Offeror, subcontractor, etc.)
Security Monitoring	
Alert Triage & Investigation	
Threat Hunting	
Incident Response	
Escalation Management	
Reporting and Metrics	
Account Management	

D.3. **Incident Detection and Response Capabilities.** Describe your capabilities and processes for detecting, investigating, responding to, and containing security incidents. Include:

D.3.1. Detection and analysis methodology, including how security events are identified, prioritized, and investigated;

D.3.2. Incident response and containment processes, including the actions the Offeror may perform directly and the actions requiring UMGC authorization.

D.3.3. Escalation and notification procedures, including communication methods and target notification timelines for critical incidents.

D.3.4. Coordination with UMGC personnel during incidents, including roles, responsibilities, and decision-making authority.

D.4. **Incident Response Scenario.** Describe your response to the following scenario:

At 2:00 AM Eastern Time, a domain administrator account is compromised, and suspicious activity is detected across multiple production systems. Describe the actions the Offeror would take during the first four (4) hours following detection of the incident. At a minimum, include:

- How the activity would be detected and initially validated;
- The triage, investigation, and severity classification process;
- The escalation and notification process, including the timing and method of communication with UMGC;
- The personnel and teams involved in responding to the incident;
- The containment and response actions that would be taken;
- The information that would be communicated to UMGC during the first four (4) hours of the incident;
- Any response actions that may be performed without prior UMGC approval and any actions requiring UMGC authorization.

D.5. **Security Operations Capabilities.** Describe your security operations capabilities and the aspects of the proposed service that distinguish it from competing managed SOC providers. At a minimum, include:

D.5.1. Threat hunting capabilities and methodology;
D.5.2. Threat intelligence sources and integration into security operations;
D.5.3. Examples of threats discovered through proactive threat hunting activities;
D.5.4. Security analytics capabilities;
D.5.5. Detection engineering and continuous improvement practices;
D.5.6. Methods used to reduce false positives and alert fatigue;
D.5.7. Automation and orchestration capabilities;
D.5.8. Reporting, metrics, and performance measurement, including service credits applicable for missed performance targets; and,
D.5.9. Unique capabilities, innovations, or differentiators relevant to the proposed services.

D.6. **Sample Deliverables.** Provide no more than one (1) example of the following deliverables from actual customer engagements. Examples should be from real customer engagements with all necessary information or details redacted.

D.6.1. monthly operational report;
D.6.2. executive reporting dashboard;
D.6.3. major incident report; and,
D.6.4. threat intelligence reports.

D.7. **Personnel.**

D.7.1. **Staffing Plan**. Provide a proposed staff plan identifying the roles required to perform the services described in the Scope of Work. For each role provide: (i) role

title, (ii) summary of responsibilities, (iii) number of personnel assigned to the role; and (iv) minimum qualifications, including relevant education, certifications, years of experience, and experience performing similar work.

D.7.2. **Mandatory Key Personnel.** Offeror must submit the qualifications and experience of the proposed Service Operations Manager, including (i) a resume, (ii) relevant certifications, (iii) a summary of experience managing similar SOC engagements; and (iv) length of time with the Offeror.

D.7.3. **Resource Continuity and Surge Support**. Describe your approach to maintaining service continuity and providing surge support. Include: (i) procedures for managing staff turnover and extended absences, (ii) cross-training and knowledge transfer practices; (iii) availability of additional resources during major incidents or periods of increased demand; and (iv) approach for maintaining required service levels during staffing changes.

D.8. **Implementation.** Describe the proposed approach for implementation and onboarding of the services. At a minimum, include:

D.8.1. Major implementation activities and milestones.
D.8.2. The Offeror's approach for onboarding, integrating, and validating monitoring across UMGC systems and environments.
D.8.3. The anticipated implementation timeline, including the estimated timeframe to achieve full operational capability.
D.8.4. Roles and responsibilities of the Offeror and UMGC during implementation.
D.8.5. Assumptions, dependencies, and risks that may affect implementation.
D.8.6. Approach for knowledge transfer, communication, and project governance during implementation.
D.8.7. In addition, Offeror must include the following table showing estimated duration for each milestone of implementation.

Milestone	Estimated Duration
Project Initiation/Planning	
Discovery & Design	
Configuration & Integration	
Testing & Validations	
Go-Live and Stabilization	

D.9. **Standards Exceptions.**

D.9.1. Offerors shall review Attachments A and B to the Scope of Work and identify any material exceptions, deviations, or limitations related to their ability to meet the standards and expectations set forth in these attachments.
D.9.2. If the Offeror has identified any material audit findings, significant deficiencies, major nonconformities, or qualified audit opinions during its most recent certification or attestation period, the Offeror shall provide a summary of the findings and the corrective actions taken.

D.10. **MBE Utilization and Fair Solicitation Affidavit & MBE Participation Schedule Form.** Complete and sign the MBE Utilization and Fair Solicitation Affidavit & MBE

Participation Schedule form which can be accessed at this link: https://content.govdelivery.com/attachments/MDDGS/2026/09/01/file_attachments/3766548/Attachment%20D-1A%20-%20Effective%209-1-26%20-%20Compressed.pdf and include it with the Technical Proposal. This form is labeled as Attachment D-1A. The information on the form may not be submitted in another format.

NOTE: Prior to submitting its request for a waiver, the Bidder/Offeror requesting a waiver should review all waiver forms (D-1B and D-1C) in Attachment D which can be access at this link: https://procurement.maryland.gov/wp-content/uploads/sites/12/2026/09/Attachment-D-MBE_Forms-Effective-9-1-26.pdf.

UMGC will only assign an MBE goal if UMGC has conducted sufficient research to confirm that there are sufficient certified MBEs that can provide subcontracting services in accordance with the contract's scope of work. If needed, UMGC's MBE Liaison will work with prime contractors/offerors who need assistance identifying one or more MBE subcontractors for the contract. The MBE Liaison can be reached at: pamela.welzenbach@umgc.edu.

D.11. **Acknowledgement of Receipt of Addenda Form.** If any addenda to the solicitation is issued prior to the due date and time for Technical Proposals, complete and sign the Acknowledgement of Receipt of Addenda Form in Appendix A and include it with the Technical Proposal.

D.12. **Proposal Affidavit:** Complete and sign the Proposal Affidavit in Appendix A and include it with the Technical Proposal.

D.13. **Offeror Profile**. Complete the Offeror Profile form in Appendix A and include it with the Technical Proposal.

D.14. **References.** Complete the References form in Appendix A and include it with the Technical Proposal.

D.15. **Insurance Documentation:** Provide a current Certificate of Insurance evidencing coverage for Commercial General Liability, Workmen's Compensation, and Cyber Security/Data Breach Insurance with the Technical Proposal. The coverage types and limits reflected in the submitted certificate are not required to meet the insurance requirements set forth in the solicitation at the time of proposal submission. However, the apparent awardee will be required to provide a Certificate of Insurance demonstrating compliance with the required insurance coverages and limits prior to contract award. See Appendix C-1 for more information.

D.16. **Maryland Living Wage Requirements Affidavit of Agreement.** Complete and sign the Living Wage Affidavit in Appendix E and include it with the Technical Proposal.

D.17. **Acknowledgement of Review of Contract:** The UMGC Contract for this Procurement will contain the provisions in Appendix C-1 as well as any additional terms required by the University or the State of Maryland. Offerors shall review Appendix C-1

and identify any requested exceptions, deviations, or concerns as part of their Technical Proposal. Failure to identify an exception in the Technical Proposal may be deemed a waiver of that exception during subsequent negotiations. By submitting a Proposal, the Offeror warrants that they have reviewed Appendix C-1 and will execute a contract: a) in substantially the same form; and b) with these terms and conditions upon request by UMGC. For accounting purposes only, UMGC will also issue a purchase order to the awarded Contractor. UMGC strongly prefers that Offerors accept the terms and conditions set forth in Appendix C-1 without modification. However, UMGC reserves the right to negotiate contract terms where permissible and consistent with applicable law, USM policy, and the best interests of the University. The University does not have the authority to accept terms and conditions that are inconsistent with Maryland law. Depending on the nature of the proposed solution and associated services, UMGC may require additional contractual provisions prior to contract execution. By submitting a Technical Proposal, the Offeror acknowledges that it has reviewed Appendix C-1 and is willing to enter into contract negotiations based substantially on the terms and conditions contained therein.

E. Modifications of Technical Proposal. Offerors may modify their Technical Proposals and upload them electronically at the UMGC Bid Locker link provided in the solicitation at any time prior to the due date and time indicated in the Solicitation Schedule. Offerors must email written confirmation of the modification, including the signature of the Offeror, to the Procurement Officer prior to the Proposal due date and time. Technical Proposals may not be modified, supplemented, cured, or changed in any way after the due date and time, unless specifically requested by the University.

F. Page Counts. The page counts below are provided solely as guidelines to assist Offerors in preparing focused and concise responses. These recommendations apply only to the narrative response for each section and do not constitute page limits.

The recommended page counts do not include:

- Required forms, affidavits, certifications, or acknowledgements;
- Appendix responses;
- Resume for Service Operations Manager;
- Sample deliverables;
- Certifications, attestations, audit reports, or other supporting documentation;
- Any materials specifically requested elsewhere in this RFP.

Section	Recommended Response Length
Transmittal Letter	1-2 pages
Company Experience (1-3 case studies)	2-6 pages
SOC Operating Model	2-4 pages
Incident Detection & Response	2-3 pages
Incident Response Scenario	2-4 pages
Security Operations Capabilities	3-5 pages
Personnel	2-4 pages
Implementation	2-4 pages
Standards Exceptions	1-2 pages

ARTICLE 2. TECHNICAL EVALUATION PROCESS

1. **Qualifying Proposals.**

   1.1. **Procurement Officer Review.** The Procurement Officer shall review each Technical Proposal for responsiveness to the requirements of the solicitation, including submission of all required forms and supporting documentation (i.e., susceptibility of award). Failure to comply with a material requirement of the solicitation may result in the Technical Proposal being deemed non-responsive. The University reserves the right to waive minor irregularities to the extent permitted by law and consistent with the best interests of the University.

   1.2. **Evaluation and Selection Committee.** All Qualifying Proposals will be reviewed by a UMGC Evaluation and Selection Committee (the "Committee") established by the Procurement Officer. As the procurement progresses, the Committee may seek input from other appropriate UMGC staff or request additional technical assistance from any other source.

2. **Technical Evaluation of Qualifying Proposals.**

   2.1. **First Phase Technical Evaluation.** Following the Procurement Officer's qualifying review, the Committee will evaluate each Technical Proposal in accordance with the following Technical Evaluation Criteria (in order of importance):

      2.1.1. Technical Approach and Service Delivery
      2.1.2. Relevant Experience
      2.1.3. Staffing and Key Personnel
      2.1.4. Implementation
      2.1.5. Standards/Contract Compliance

   2.2. Minor irregularities contained in Technical Proposals, which are immaterial or inconsequential in nature, may be waived wherever it is determined to be in the University's best interest and when permitted by law. The decision for progressing in the procurement process will be made based on the strengths, weaknesses, advantages, and deficiencies that the Technical Proposals represent.

   2.3. **Shortlisting:** In accordance with the Technical Evaluation Criteria set forth above, a shortlist of qualified proposals may be established after the initial technical evaluation. If a shortlist is established, only shortlisted Offerors would continue in the evaluation process. Offerors not shortlisted shall be so advised.

3. **Oral Presentations/Discussion Sessions.**

   3.1. **Purpose:** Based on the Committee's initial technical evaluation, the University may invite, without cost to itself, Offerors to an oral presentation/discussion session ("Discussion Session"). The purpose of the Discussion Session is as follows:
      3.1.1. To discuss/clarify any and all aspects of the Technical Proposal;
      3.1.2. To allow the University to meet Offeror personnel; and
      3.1.3. To provide an opportunity to clarify the scope of services for the intended contract and discuss any items addressed in the Technical Proposal that may require additional clarification.

3.2. **Format:** The Discussion Session will be informal; the University is not interested in a sales presentation by executives and business development staff. Rather, we are seeking an interactive discussion with the Offeror. The use of PowerPoint (or similar technology) is encouraged. The Discussion Session will be virtual and no more than 60 (sixty) minutes in length. Following the Discussion Session, additional follow-up and/or clarification documentation may be requested of the Offeror.

3.3. **Date:** The times and dates for the Discussion Session(s) will be scheduled upon completion of the initial technical evaluation; however, it is anticipated that the Discussion Session(s) will be conducted on the times and dates listed per the Solicitation Schedule. Proposers are therefore advised to set this(ese) date(s) aside in its (their) entirety on the calendars of the appropriate personnel.

4. **Second Phase Technical Evaluation.**

4.1. **Criteria:** Following the Discussion Session, a second phase technical evaluation will be conducted. The Committee will re-evaluate all criteria, incorporating assessment of the Discussion Session and, at its sole discretion, outcome of reference checks. The University reserves the right to decide that an Offeror is not shortlisted prior to completing reference checks. The order of Technical Evaluation Criteria remains the same.

4.2. **Process:** Further shortlists may result as the procurement progresses. At each phase of the process, those Offerors that do not remain shortlisted will not progress in the procurement. All Proposers will be notified of the results of the Technical Evaluation as they pertain to their respective Technical Proposals. It is UMGC's intent to incorporate references prior to establishing the final shortlist of proposals. Once a final shortlist of proposals is established, the Committee will rank the remaining Technical Proposals from highest to lowest.

(End Section III. Article 2. Technical Evaluation Process)

ARTICLE 3. PRICE PROPOSAL REQUIREMENTS

1. **General Requirements.** The Offeror shall submit a complete Price Proposal containing all pricing, information, forms, assumptions, and supporting documentation required by this solicitation. Refer to Section I.5.2 of this solicitation for the submission instructions. The Price Proposal must provide all pricing necessary to perform the services described in this solicitation.

2. **Evaluation.**

   2.1. Price Proposals will be evaluated separately from Technical Proposals. Price Proposal evaluation will not be performed for an Offeror whose Technical Proposal is determined to be unacceptable and/or for any Offeror who does not remain shortlisted after technical evaluation.

   2.2. Price Proposals will be evaluated based upon the Offeror's overall cost to provide the required goods and/or services, the reasonableness and competitiveness of proposed pricing, the completeness of the pricing proposal, and any pricing assumptions or risks that may affect the total cost of ownership.

   2.3. The University is not required to select the lowest-priced proposal and will consider the relationship between technical merit and price in determining overall best value.

   2.4. Following the initial evaluation, the University may, in its sole discretion, request Best and Final Price Proposals (“BAFO”).

   2.5. The Committee will establish a financial ranking of the Price Proposals and/or BAFOs from lowest to highest total offers.

3. **Price Form.** Each Offeror shall complete and submit the Price Form attached as Appendix B in Microsoft Excel format. Do not alter the Price Form. The Price Form is to be signed and dated where requested by an individual who is authorized to bind the Offeror to the prices entered on the Price Form. The Price Form must be submitted in the Microsoft Excel format as provided. Please do not submit a PDF.

   3.1. Tab labeled “Costs”. Offerors shall provide 1) a fixed price for the One-Time Implementation Services and 2) a fixed monthly and annual price for the Managed SOC Services described in the solicitation, including all monitoring, investigation, escalation, reporting, governance, and continuous improvement activities required to support the University's environment.

   3.2. Tab labeled “Implementation Breakdown”. Offerors shall provide the Labor Category Title, level of effort in hours, and hourly rate for each position for each phase listed in Tab 2. Include any assumptions.

   3.3. Tab labeled “Rate Card”. Offerors shall provide a rate card identifying all labor categories that may be utilized to perform As-Needed Services during the Contract term. For each labor category, Offerors shall provide: (a) the labor category title; (b) minimum qualifications; and (c) a fully burdened hourly rate. Proposed labor categories

may include resources used for incident response surge support, digital forensics, threat hunting, security engineering, security architecture, project management, and other cybersecurity consulting services. All rates shall assume performance in a remote work environment unless otherwise identified by the Offeror.

4. **Price Proposal Narrative.** In addition to the completed Price Form (Excel Sheet), Offerors shall submit a narrative that explains the proposed pricing. Identify:

   4.1. All assumptions used in developing pricing, including, but not limited to:

      4.1.1. Staffing assumptions
      4.1.2. Technology assumptions
      4.1.3. Log volume assumptions
      4.1.4. Asset or endpoint assumptions
      4.1.5. UMGC responsibilities
      4.1.6. Third-party dependencies

   4.2. What incident response activities are included in the monthly managed SOC fee.

   4.3. Whether any incident response hours are included annually.

   4.4. What events trigger additional charges.

   4.5. Whether after-hours, weekends, and holidays are billed at different rates.

5. **Pricing Conditions**.

   5.1. The Rate Card shall establish the labor categories and rates available for use under the resulting Contract**.**

   5.2. Additional labor categories not included in the Rate Card may be proposed and are subject to negotiation and approval by UMGC.

   5.3. The Offeror shall disclose all known fees and charges associated with the proposed services. Failure to disclose a recurring fee, minimum commitment, or other material pricing component may be considered during price evaluation and contract negotiations.

(End Section III. Article 3. Price Proposal Requirements)

ARTICLE 4. FINAL EVALUATION, RANKING AND SELECTION

1. **Recommendation of Award or Further Discussions.** The Committee may recommend a Proposer for contract award(s) based upon the Offeror's Technical Proposal and Price Proposal without further discussion. However, should the Committee find that further discussion would benefit the University and the State of Maryland, the Committee may recommend such discussions to the Procurement Officer. Should the Procurement Officer determine that further discussion would be in the best interest of the University and the State, the Procurement Officer shall establish procedures and schedules for conducting discussions and will notify responsible Offerors.

2. **Final Ranking and Selection.**

   2.1. Process: Following evaluation of the Technical Proposals and the Price Proposals (and Best and Final Offers, if applicable), the Evaluation and Selection Committee will make an initial overall ranking of the Proposals and recommend to the Procurement Officer the award of the contract(s) to the Offeror whose Proposal(s) is (are) determined to be the most advantageous to the University and the State of Maryland. The decision of the award(s) of the Contract will be made at the discretion of the Procurement Officer and will depend on the facts and circumstances of the procurement. All Offerors will be notified of the award(s) selection.

   2.2. **Basis for Award:** Technical merit will have a greater weight than cost in the final ranking. Award may be made to the Offeror with a higher technical ranking even if its Price Proposal is not the lowest. The Procurement Officer retains the discretion to examine all factors to determine the award of the contract. The goal is to contract with the Offeror(s) that would best meet the needs of the University as set forth in the RFP.

   2.3. **Negotiations:** The University may select for award one or more Offeror(s) to negotiate the terms and conditions of the Contract. The University reserves the right to make an award with or without negotiation.

3. **Debriefing.**

   3.1. **Request:** Unsuccessful Offerors may request a debriefing. A request must be submitted in writing to the Procurement Officer within ten (10) days after the date on which Offeror knows, or should have known, that its Proposal was unsuccessful. Debriefings shall be conducted at the earliest feasible time.

   3.2. **Discussion:** Debriefings shall be limited to discussion of the Offeror's Proposal only and shall not include a discussion of a competing Offeror's Proposal. The debriefing may include information on areas in which the unsuccessful Offeror's Proposal was deemed weak or insufficient. The debriefing may not include discussion or dissemination of the thoughts, notes, or ranking from an individual Evaluation and Selection Committee Member. A summary of the Procurement Officer's rationale for the selection may be given.

(End Section III. Article 4. Final Evaluation, Ranking and Selection)

APPENDICES

The documents listed as appendices below are incorporated into the solicitation are available as separate attachments on eMaryland Marketplace and UMGC's Bid Locker platform.

Appendix A – Forms

A-1. Offeror Qualification: Information Security Certification

A-2. Acknowledgement of Receipt of Addenda Form

A-3. Bid/Proposal Affidavit

A-4. Offeror Information

A-5. References Form

Appendix B – Price Proposal Form

B-1. Price Proposal Form

Appendix C – Contract Terms and Conditions

C-1. Professional Services Contract

C.2. Contract Affidavit - The Contract Affidavit included in this solicitation is a sample, for information purposes only. If a contract is awarded as a result of this procurement, only the successful offeror must complete the Contract Affidavit; do not enclose it with the Technical Proposal.

Appendix D – Electronic Funds Transfer Schedule

Appendix E – Maryland Living Wage Requirements Affidavit of Agreement

Appendix M – Minority Business Enterprise (MBE) Participation Goal

Appendix S – Solicitation Terms and Conditions