Question Number	Question Text	Response / Answer
1	How large is UMGC's internal Security Operations team and what hours does it cover?	UMGC's Security Operations team consists of approximately 5-10 personnel and maintains 24x7 security operations coverage.
2	Is there an incumbent MSSP, and is this a replacement or a new service?	This is a new service.
3	Please identify the current SIEM platform, along with approximate daily log ingestion (GB/day or EPS) and the number of log sources currently onboarded.	Currently UMGC utilizes Exabeam as our SIEM (New-Scale Fusion SIEM), with about 115 GB daily ingestion and 235 currently onboarded log sources. We are using Exabeam's native SOAR and UEBA capabilities.
4	Is there a planned backlog of new log sources during the term, or a cap on how many count as in scope for the fixed fee?	Yes. UMGC anticipates onboarding additional log sources during the contract term and currently has a planned backlog of approximately 100 log sources that are expected to be in scope. Offerors should account for the onboarding, integration, and monitoring of these sources in their proposed solution and clearly identify any assumptions, limitations, capacity thresholds, or pricing considerations associated with managing additional log sources over the term of the agreement.
5	Will UMGC consider proposals that use the Offeror's own SIEM or MDR platform, either as an alternative or alongside the existing tools? Or must all services run on UMGC's current platforms?	At this time our preference is to utilize our platforms. Alternatively, we are willing to use the Offeror's tools, alongside our existing tools.
6	If you have SOAR, do you have custom playbooks? If yes, what is approx. number? If not, is this desired?	Yes, we have five (5) custom playbooks.
7	Should all four quarterly tabletops be executive-level, technical, or a mix? Are they virtual or on-site? Should the quarterly incident response tabletop exercises and after-action reviews in Section II §4.2.5 be priced as remote facilitation, or does UMGC expect any of them to be conducted on-site in Adelphi?	At least one tabletop should be executive-level, and the rest may be technical. Preference is the executive one be done on-site but not a requirement. Offerors should identify any assumptions related to travel and onsite facilitation in their price proposals.
8	Does UMGC expect full investigation and remediation of Critical incidents under the monthly fee, or coordination only, with forensics billed separately at rate-card rates? Is there an existing IR retainer firm?	The University expects Offerors to clearly describe the incident response services included in the proposed monthly fee, including any limitations, assumptions, exclusions, service thresholds, response volumes, or labor-hour restrictions. Offerors should also identify any services that would require separate authorization and additional fees, such as digital forensics, malware analysis, recovery assistance, incident remediation support, surge support, or other specialized cybersecurity services. The University will evaluate each Offeror's proposed service model, including the scope of services included in the monthly fee and any separately priced services. The University does not have a current IR retainer firm.

Question Number	Question Text	Response / Answer
9	Under Section II.7.1 (Minimum Qualifications), the RFP requires offerors to possess either a current	Pursuant to Section II.7.1, the required ISO/IEC 27001 certification or SOC 2 Type II attestation must be held by the Offeror submitting the proposal. As stated in Section II.7, the experience of subcontractors, affiliates, parent companies, technology partners, or other third parties will not be considered in determining whether an Offeror satisfies the minimum qualification requirements. The University will accept proposals that include subcontractors, partners, or other third parties in the delivery of the proposed services. The resulting contract, if awarded, will be between the University and the Offeror, and the Offeror shall remain fully responsible for contract performance, service delivery, subcontractor management, and compliance with all solicitation and contract requirements. Offerors are also reminded that the solicitation includes a Minority Business Enterprise (MBE) subcontracting goal of three percent (3%) of the total contract value. Accordingly, the use of subcontractors is contemplated under the solicitation; however, subcontractor qualifications may not be substituted for the Offeror's minimum qualification requirements.
10	If an Offeror relies on a subcontractor, partner, or underlying technology provider that holds a SOC 2 Type II attestation, while the Offeror is currently undergoing its own SOC 2 audit, would the University accept the underlying provider's attestation along with evidence of the Offeror's independent security assessment and a commitment to provide the Offeror's SOC 2 attestation upon completion of the audit?	No. The Offeror must satisfy the minimum qualification requirements as of the Technical Proposal due date.
11	Section 4.3.1 identifies UMGC's existing security technology categories, including SIEM, EDR, IDS/IPS, DLP, network/perimeter security, and vulnerability management, but states that the specific platforms will be shared with the awarded Contractor. Given that Offerors are required to propose a staffing model, personnel qualifications and certifications, technical approach, integrations, and experience performing similar work, will UMGC identify the currently deployed products/platforms within its security technology stack prior to proposal submission so Offerors can propose personnel with appropriate platform-specific experience and develop an informed technical and pricing approach to support a valuable response?	Currently UMGC utilizes Exabeam as our SIEM (New-Scale Fusion SIEM), with about 115 GB daily ingestion with 235 currently onboarded log sources. Offerors should assume 4,100 endpoints/servers and 150,000 monitored users. These numbers are not expected to change significantly during the term. MS Defender is one EDR tool. We also have TrendAI.
12	To enable Offerors to appropriately size the proposed 24x7 SOC operating model, staffing levels, implementation effort, and fixed-price managed SOC services, will UMGC provide approximate current-state environment scale, including the number of users, endpoints, servers and applicable compute systems operating systems, network/security devices, cloud (AWS/GCP/Azure) and data center environments? The geographic locations were provided but exclude the true Enterprise scope.	See Response to Question No. 11.

Question Number	Question Text	Response / Answer
13	Does UMGC have a preferred or typical partner it uses when purchasing, such as a reseller or contract vehicle?	The University does not have a preferred reseller, distributor, channel partner, or contract vehicle for this solicitation. Offerors may propose their preferred teaming arrangement, reseller, or authorized channel partner, provided the proposal clearly identifies all parties and the contractual relationship among them. Any proposed arrangement must comply with the requirements of the solicitation. If the successful Offeror intends to provide services through a reseller or channel partner, the proposal should clearly identify the role of each entity and any applicable authorizations or certifications.
14	What is the renewal date of your existing SIEM?	UMGC's existing security technology contracts and renewal timelines are not relevant to proposal preparation. UMGC does not plan to replace our current SIEM at this time.
15	How many days is your current hot log storage?	45 days.
16	What is the list of devices currently logging to UMGC's SIEM?	Current log sources include identity and access management platforms, endpoint security platforms, vulnerability management tools, firewalls, network security devices, cloud infrastructure services, operating systems, productivity platforms, and other enterprise applications.
17	Section II §3.1.1 and §4.3.1 state that the Contractor will use UMGC's approved security monitoring platforms and that the specific platforms will be shared with the awarded Contractor. Can UMGC identify the SIEM platform it uses today? Can UMGC also confirm whether SOC work must be performed entirely within UMGC's SIEM, or whether an Offeror may use its own analytics or investigation tooling alongside it, with UMGC's SIEM remaining the system of record?	Currently UMGC utilizes Exabeam as our SIEM. At this time our preference is to utilize our platforms. Alternatively, we are willing to use the Offeror's tools, alongside our existing tools.
18	Can UMGC provide approximate counts of users (staff and students), endpoints, and servers; average daily ingestion into the SIEM (GB/day or EPS); and the number of log sources currently onboarded? Can UMGC also confirm whether its Europe and Asia locations are in scope for monitoring?	Yes, Europe and Asia are included in the scope. See Response to Question No. 11.

Question Number	Question Text	Response / Answer
19	Attachment B (Service Levels and Performance Metrics) raises three related points that affect how Offerors price and commit to the service levels. (a) The MTTD and MTTR targets in §3 read "≤ 90%" of incidents within the target time, while the §5 service credit tables apply no credit at "90% or greater." Can UMGC confirm that the targets are at least 90% of incidents within the target time? (b) §5.2–5.4 tie corrective-action and material-breach triggers to "any Critical Service Level," but the term is not defined. Which service levels does UMGC consider Critical Service Levels? (c) §2 defines MTTD as the time from the occurrence of a security event to its detection. Will UMGC accept measuring MTTD from the event's arrival in UMGC's SIEM, since time before ingestion is outside the Contractor's visibility, and confirm that MTTR measures the initiation of response and containment activities, not their completion?	(a) The references to "≤ 90%" in Attachment B are typographical errors. The intended performance target for MTTD and MTTR is ≥ 90% of applicable incidents meeting the specified response times. See Addendum #1 to the RFP which formally revises the targets in the table. (b) UMGC has not designated specific Service Levels as Critical Service Levels. Offerors are expected to propose an appropriate Service Level framework, including identification of any Service Levels they consider critical and any associated service credit methodology, subject to UMGC review and acceptance. (c) Yes, see Addendum #1 to the RFP which formally revises the defintions of MTTD and MTTR.
20	Can a MD-certified MBE partner on multiple submitted proposals for this opportunity?	Yes.
21	UMGC has identified approximately 150,000 monitored users. Can UMGC provide a breakdown of this population by administrative/staff, faculty, and students? Additionally, are all 150,000 users expected to receive the same level of security monitoring and incident response, or are there different requirements based on user type?	Staff: 4k Faculty: 7k Student: 100,000 Not consistent monitoring but part of the risk calclus as we have some accounts as "inactive" due to whether they are active for a particular term.
22	Attachment A §3 (Artificial Intelligence Preferred Standards) refers to learning objectives, instructional content, and program outcomes, and Appendices C-2, D, and S carry the header "UMGC RFP #92303 – Custom AI-Enabled Content Development." Can UMGC confirm that these documents apply to RFP #92340 as written, and indicate how Offerors should address Attachment A §3 for a managed SOC service?	Addendum #1 addresses this discrepancy.
23	Section II §4.1.6–4.2.8 and §4.3.6 require the Contractor to review and update UMGC's existing SOC Operations Runbook, Incident Severity and Escalation Matrix, Incident Response Plan, playbooks, and SIEM Detection Catalog. Can UMGC indicate approximately how many playbooks and detection rules are currently in place, so Offerors can size the annual review effort?	UMGC has identified that it currently has five (5) custom playbooks. Offerors should size the annual review effort based on the scope requirements to review, update, maintain, and document these materials.
24	The Price Form signature page states that no change in Key Personnel is allowed without a contract amendment, while Appendix C-1 §2.3–2.4 permits substitution for termination of employment, leave, illness, and similar causes, subject to UMGC review. Which provision governs?	UMGC does not view these provisions as conflicting. Appendix C-1 §2.3-2.4 identifies circumstances under which the Contractor may request a substitution of Key Personnel, including situations such as termination of employment, leave of absence, promotion, illness, or inability to continue performing the required duties. Any proposed substitution remains subject to UMGC review and approval and must satisfy the qualification requirements set forth in Appendix C-1. As stated in the Price Form, changes to Key Personnel must be formalized through a contract amendment.

Question Number	Question Text	Response / Answer
25	Section II §5.1 states that no return of UMGC data is anticipated because UMGC data remains in UMGC's systems, while Appendix C-1 §11.10 requires five-year record retention followed by return and deletion of UMGC Data. Can UMGC confirm that §11.10 applies only to records the Contractor actually holds, such as reports, case records, and working papers?	Appendix C-1 §11.10 applies to any UMGC Data maintained, stored, or retained by the Contractor in connection with the Services. Any UMGC Data in the Contractor's possession, such as reports, tickets, case files, investigation records, working papers, evidence, or exported data, must be returned and/or destroyed in accordance with the contract.
26	Appendix C-1 §10.24–10.25 (acceptance testing, WCAG 2.1 AA, VPAT and HECVAT) apply to Digital Properties made available to students, employees, or the public. Do these sections apply to Contractor portals and dashboards used only by UMGC security staff?	Yes.
27	Can UMGC provide vendors with the number of notable alerts you receive each month? Our definition of a notable alert is a unique alert or event requiring human analysis or investigation.	300
28	There are a few terms and conditions in the main RFP but the majority reside in Appendix S and Appendix C-1. Can UMGC clarify if exceptions to the 2 appendices need to be captured in the Transmittal Letter? Or can vendors submit separate redlined versions of Appendix C-1 or Appendix S?	Requested exceptions, deviations, or concerns regarding Appendix C-1 and Appendix S should be identified in the Technical Proposal/transmittal materials as provided in the RFP.
29	Can UMGC clarify if Attachment M needs to be included as part of the final submission or is it primarily designed to be used as a guide for how vendors are to approach filling out Attachment D-1A?	Appendix M provides information about the MBE goal and the requirements. Attachment D-1A is the MBE form expressly required to be completed and included with the Technical Proposal.
30	Please provide the estimated budget or funding range allocated for this requirement, if available.	UMGC is not releasing an estimated budget or funding range for this solicitation. Offerors should submit their most competitive pricing based on the requirements set forth in the RFP and all related addenda.
31	What is the expected frequency, cadence, and deliverable format for proactive threat hunting campaigns (e.g., monthly vs. quarterly hypothesis-driven hunts)?	We envision quarterly hypothesis-driven but also some will be situational depending on the threat landscape we are dealing with.
32	Could the University provide indicative examples or historical task profiles for the ad-hoc projects expected under the T&M Rate Card labor categories (e.g., Threat Hunting, Security Engineering, IR Surge Support)?	Offerors should price the Rate Card based on the labor categories and assumptions they believe are necessary to support the solicitation, recognizing that UMGC does not guarantee any minimum utilization of As-Needed Services.
33	To ensure proper resource planning, bench readiness, and Rate Card pricing alignment, could the University clarify the expected mobilization SLA (turnaround time) for deploying resources under ad-hoc T&M requests, and whether there is an anticipated monthly baseline volume of T&M hours or a minimum billable duration per task?	Such work will be authorized by UMGC, subject to mutually agreed work assignments, and, unless otherwise authorized in writing, performed on a time-and-materials basis using the contract rates.
34	What IT Service Management (ITSM) or ticketing platform is currently utilized by UMGC SecOps teams (e.g., ServiceNow, Jira Service Management, etc? Does UMGC expect bi-directional API integration between the MSSP's SOC platform and UMGC's internal ITSM tool or will the MSSP operate directly within UMGC's ticketing tenant?"	UMGC uses ServiceNow. We can manage via bi-directional API integration as we already do that with other MSSP services.
35	Can we provide anonymized references?	Offerors may anonymize client names in case studies when disclosure is restricted, consistent with the RFP. However, references submitted for evaluation must identify the client and provide sufficient contact information for UMGC to conduct reference checks. Such reference information may be submitted as confidential.

Question Number	Question Text	Response / Answer
36	Please provide an inventory of the security tools and technologies currently deployed within the University environment, including SIEM and EDR.	Currently UMGC utilizes Exabeam as our SIEM (New-Scale Fusion SIEM), with about 115 GB daily ingestion with 235 currently onboarded log sources. Offerors should assume 4,100 endpoints/servers and 150,000 monitored users. These numbers are not expected to change significantly during the term. MS Defender is one EDR tool. We also have TrendAI.
37	Please provide the current data ingestion volume into the SIEM platform, including average daily ingest (GB/day or events per second), the primary log sources being collected, and any retention requirements.	UMGC has identified approximate SIEM ingestion of 115 GB per day. Current log-source types include identity and access management platforms, endpoint security platforms, vulnerability management tools, firewalls, network security devices, cloud infrastructure services, operating systems, productivity platforms, and other enterprise applications.
38	Does the University require the SecOps Manager role to be a dedicated, full-time resource?	Yes, the resource is expected to be dedicated to the UMGC scope of work and service.
39	Attachment B 2 measures MTTD from when a security event occurs. Will UMGC instead start the MTTD clock when telemetry reaches the SIEM or an alert is generated? Will time spent waiting on UMGC approvals, or on delayed or missing telemetry, be excluded from MTTD and MTTR? Also, 5.2 and 5.4 refer to "Critical Service Levels" without defining the term. Which service levels does UMGC mean?	See Response to Question #19 above.
40	Instructions state "Offerors shall provide one (1) to three (3) case studies illustrating the Offeror's ability to deliver services comparable to those requested by UMGC." Please clarify the definition of comparable, will comparable be judged by size of organizations supported, complexity in number of sites supported, geographic complexity (supporting offices outside of the US)?	For purposes of this solicitation, 'comparable' should be understood to mean engagements similar to the services requested by UMGC in scope, complexity, and operating environment. The RFP specifically points Offerors to factors such as scope of services, whether the engagement included a new SOC implementation, duration, client environment characteristics (including approximate users, endpoints, monitored assets, and geographic distribution), measurable outcomes, and supported regulatory/security frameworks. No single factor is controlling.
41	Please clarify regarding format and length for price proposal narrative?	UMGC does not prescribe a page limit for the Price Proposal narrative. Offerors must submit the Excel Price Form and a narrative explaining the proposed pricing, including the assumptions and pricing elements identified in Article 3, Section 4.
42	SOC Technology Platform: Does UMGC expect the selected provider to operate and optimize UMGC's existing SIEM and security technology stack, or may offerors propose a provider-managed SIEM/SOAR/XDR platform that integrates with and complements UMGC's existing security investments?	UMGC’s preference is for the selected provider to utilize and operate within UMGC’s current platforms. However, UMGC is willing to consider Offeror tools proposed alongside the existing environment, provided the proposal meets the requirements of the solicitation and clearly explains the approach.

Question Number	Question Text	Response / Answer
43	Existing Platform Integration: For existing security analytics platforms, including Exabeam, does UMGC expect the selected provider to integrate with and operate these platforms, or may offerors propose consolidation of selected detection, correlation, and response capabilities where operational or security benefits can be demonstrated?	UMGC expects the selected provider to support and optimize the existing approved security platforms, and the University does not plan to replace its current SIEM at this time. Offerors may describe alternative or complementary approaches, but UMGC's preference is to leverage current platforms.
44	Automated Response and Remediation: What level of incident response authority will UMGC delegate to the selected provider? Specifically, may offerors propose pre-approved automated containment and remediation playbooks for defined incident scenarios, with human validation and escalation for higher-risk actions?	Yes. Offerors may propose pre-approved automated containment and remediation playbooks for defined incident scenarios, provided the proposal clearly identifies which actions may be taken without prior UMGC approval and which actions require UMGC authorization, as well as the related validation, escalation, and notification processes.
45	Telemetry and Environment Sizing: To support accurate solution sizing and pricing, can UMGC provide the approximate daily log ingestion volume and the number of endpoints, servers, network and security devices, identity sources, cloud workloads, applications, and other principal telemetry sources expected to be within scope?	See Response to Question No. 11.
46	Incident Response Roles and Responsibilities: For confirmed security incidents, please clarify the expected division of responsibilities between the selected SOC provider and UMGC personnel across L1/L2/L3 investigation, containment, remediation, recovery, evidence preservation, and stakeholder communication.	UMGC does not prescribe a fixed L1/L2/L3 split. In general, the MSSP is responsible for security monitoring, detection, triage, escalation, incident response support, reporting, and operational recommendations. UMGC is responsible for providing access, information, resources, timely decisions and approvals, and engaging appropriate stakeholders. Incident management, remediation coordination, and continuous improvement are shared responsibilities.
47	Exabeam licensing and platform costs. Please confirm whether UMGC will retain responsibility for Exabeam licensing, storage, retention, infrastructure, platform support, and any incremental costs associated with the current 115 GB daily ingestion volume and the approximately 100 additional log sources planned for onboarding. If the contractor is expected to include any Exabeam licensing, storage, professional services, or consumption costs in its fixed fee, please identify those requirements.	UMGC will retain responsibility for Exabeam licensing and associated costs.

Question Number	Question Text	Response / Answer
48	1. Section II.4.3.1 (Tooling): Please identify the SIEM, EDR, IDS/IPS, DLP, and vulnerability management platforms in use (vendor, product, licensing tier). Does UMGC expect the MSSP vendor to bring any additional tooling? 2. Section III, Article 3, #4.1 (Environment Size): What are the approximate daily log volume (GB/day or EPS), number of users, number of endpoints/monitored assets, and number of log sources onboarded today and planned for Year 1? 3. Attachment B, #5.2-5.4 (Service Levels): Please define "Critical Service Level." Does it refer only to the Critical-severity MTTD/MTTR targets?	1. Tooling is identified above. 2. Environment size is identified above. 3. UMGC has not designated specific Service Levels as Critical Service Levels. Offerors are expected to propose an appropriate Service Level framework, including identification of any Service Levels they consider critical and any associated service credit methodology, subject to UMGC review and acceptance. The language referenced in Attachment B - Section 5 is: "*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:* "
49	Given the scope and complexity of this procurement, would the State consider a four (4) week extension to the proposal submission deadline to allow Offerors to submit more complete and competitive responses? If an extension is granted, does the State anticipate maintaining the current evaluation and award timeline, or adjusting key milestone dates accordingly?	Pursuant to Addendum #2, the technical and price proposal due date is extended to Thursday, November 19 by 10:00 am ET.
50	Please confirm whether Offerors may submit redlined exceptions to the State's Standard Terms and Conditions as part of their proposal.	Offerors should identify any requested contract exceptions, deviations, or concerns in their Technical Proposal/transmittal materials as provided in the RFP.
51	Will commercially reasonable and risk-balanced contract redlines be reviewed and considered during the evaluation and negotiation process?	UMGC strongly prefers that Offerors accept the contract terms as written, but the RFP states that UMGC reserves the right to negotiate contract terms where permissible and consistent with applicable law and policy. Any requested exceptions should be clearly identified in the Technical Proposal.
52	Please confirm whether the unlimited liability provisions in the Standard Contract Terms are negotiable.	UMGC does not pre-approve negotiation of any specific liability provision. UMGC strongly prefers acceptance of Appendix C-1 as written, but reserves the right to negotiate contract terms, where permissible, in the best interests of the University and consistent with applicable law and USM policy.
53	Would the State consider a mutual limitation of liability cap (e.g., tied to a multiple of annual contract value), with customary carve-outs for data breach, willful misconduct, and statutory violations?	See UMGC response to Question No. 51 and No. 52.
54	Are offshore or nearshore resources permitted for any portion of the services, provided all security, data residency, and compliance requirements are met?	Yes, except as revised for Key Personnel. Offerors should identify the locations from which the SOC services will be delivered, including any offshore or nearshore resources. Per Addendum #1, the Service Operations Manager must be physically located within the United States throughout the contract term.

Question Number	Question Text	Response / Answer
55	Section II says the specific platforms will be shared with the awarded Contractor, but the Price Form asks for a fixed monthly fee before then. Can UMGC share, before proposals are due, the SIEM and EDR products in use, the number of monitored users, endpoints, and servers, daily log volume, average and peak alert counts, and the growth UMGC expects over the term?	See Response to Question No. 11. Average number of peak alert counts is 200.
56	Can you please clarify what is included in the scope of the monthly fee? Additionally, can you please provide examples of separately authorized work?	The University's expectation is that the Contractor will provide the Managed SOC Services described in the RFP, including monitoring, detection, alerting, investigation, analysis, escalation, and response coordination activities within the scope of the managed service. Offerors must clearly identify any assumptions, limitations, thresholds, exclusions, or service-level constraints applicable to their proposed monthly fee. As-Needed Services and One-Time Projects are intended to address services beyond the routine Managed SOC Services scope that may be requested by the University. Examples may include specialized cybersecurity consulting, security assessments, dedicated threat hunting engagements, digital forensics, malware analysis, recovery assistance, surge staffing, major one-time integration efforts, and other project-based services. Offerors should clearly identify any assumptions regarding services included in the monthly fee and any services they consider separately authorized work.
57	Apart from the U.S. or nearshore allowance for the Service Operations Manager, are there limits on where analysts may be located, or on offshore or subcontractor access to UMGC systems and data?	See Addendum #1 to the RFP which formally revises the requirements for the Service Operations Manager. The Offeror must certify that it is not engaging in investment activities in Iran as described in State Finance & Procurement Article, Section 17-702, Annotated Code of Maryland. Any personnel providing services under the Contract must work from secured and compliant equipment supplied by the Offeror (or the subcontractor). The awarded Contractor will be expected to provide security and compliance reporting on a monthly basis.

Question Number	Question Text	Response / Answer
58	Will UMGC accept a reseller as the prime and solution provider partner model for this solicitation, o	Yes. UMGC will accept proposals in which the Offeror serves as the prime contractor and utilizes subcontractors, partners, resellers, or other third parties in the delivery of the proposed services. The resulting contract, if awarded, will be between UMGC and the Offeror, and the Offeror shall remain fully responsible for contract performance, service delivery, subcontractor management, and compliance with all solicitation and contract requirements. Offerors are reminded that the solicitation includes a Minority Business Enterprise (MBE) subcontracting goal of three percent (3%) of the total contract value. Accordingly, the use of subcontractors is contemplated under this solicitation. However, pursuant to Section II.7.1, the Offeror submitting the proposal must independently satisfy the minimum qualification requirements. The qualifications of subcontractors, affiliates, parent companies, technology partners, solution providers, resellers, or other third parties will not be considered in determining whether the Offeror meets the minimum qualifications.
59	Additional log-source onboarding schedule UMGC identified approximately 100 additional log sources expected to be onboarded during the contract term. Does UMGC have an anticipated deployment schedule or annual onboarding target for these sources? Please also clarify whether the backlog primarily consists of standard supported connectors or whether offerors should expect custom parsers, APIs, agents, collectors, or other custom integration development.	UMGC has indicated that approximately 100 additional log sources are expected to be onboarded during the contract term. UMGC does not have a deployment schedule, annual target, or a breakdown between standard and custom integrations. Offerors should identify any assumptions, limitations, or pricing considerations related to onboarding those sources.
60	Current Exabeam content and operational responsibility Please provide the approximate number of active correlation rules, detection models, dashboards, reports, and automation workflows currently maintained in Exabeam. Please clarify whether the selected contractor will have administrative authority to create, modify, tune, disable, and retire this content directly, subject to UMGC's change-management requirements.	The Contractor is expected to review, update, maintain, and document the SIEM Detection Catalog, use cases, rules, playbooks, and related operational documentation, which indicates the selected Contractor will be expected to perform those functions within UMGC's governance and change-management processes.
61	Asset and critical-system prioritization Of the approximately 4,100 endpoints and servers and 150,000 monitored users, can UMGC provide an approximate count of privileged identities, critical servers, externally facing systems, cloud workloads, and other assets classified as high value or mission critical? If these counts are not available before proposal submission, should offerors assume that asset classification and criticality mapping will be completed jointly during implementation?	Offerors should use the provided planning assumptions—approximately 4,100 endpoints/servers and 150,000 monitored users—and may assume that detailed asset classification and criticality mapping will be refined jointly during implementation and onboarding.

Question Number	Question Text	Response / Answer
62	Geographic and data-handling requirements Because Europe and Asia are included in scope, are there any location-specific requirements governing where SOC analysts may access UMGC telemetry, where security data may be processed or stored, or whether services must be delivered exclusively by U.S.-based personnel? Please identify any applicable data-residency, export-control, privacy, or personnel-location restrictions that offerors should incorporate into their staffing and technical models.	Offerors must describe where services will be delivered, maintain appropriate safeguards and least-privilege access controls, and comply with the applicable institutional, regulatory, and security requirements in the solicitation. Per Addendum #1, the Service Operations Manager must be physically located in the United States throughout the contract term.
63	Implementation access and transition readiness At contract initiation, will UMGC provide the selected contractor with access to existing Exabeam architecture documentation, connector inventories, detection content, playbooks, runbooks, escalation procedures, asset inventories, service-account requirements, and historical alert and incident data? Please identify any known access, dependency, or change-control constraints that offerors should account for in the implementation schedule.	UMGC will provide the awarded Contractor with the access, information, and resources reasonably required to perform the services. The RFP does not enumerate every implementation artifact or access dependency in advance, so Offerors should assume onboarding will require coordination around access provisioning, documentation transfer, approvals, and change-management processes during implementation.
64	UMGC indicates its Security Operations team maintains 24x7 coverage. Does UMGC expect the Contractor to provide full 24x7x365 analyst coverage independent of UMGC staff, or to augment UMGC coverage during specific hours or for specific alert tiers?	UMGC expects the MSSP to deliver end-to-end managed SOC services, including 24x7x365 monitoring and analysis, incident detection, triage, escalation, containment, and response coordination. While UMGC maintains its own Security Operations team, the RFP does not limit the Contractor's role to augmentation during certain hours or specific alert tiers.
65	Please identify which Exabeam product UMGC operates (for example, the cloud-native New-Scale Security Operations Platform, Exabeam Fusion, or LogRhythm SIEM) and whether it is SaaS or self-hosted.	Currently UMGC utilizes Exabeam as our SIEM (New-Scale Fusion SIEM).
66	(a) What is UMGC's target date for full operational capability? (b) The RFP references NIST SP 800-171 and CMMC. Are environments containing Controlled Unclassified Information in scope for SOC monitoring under this contract?	(a) UMGC is not able to specify a fixed target date for full operational capability at this point in the process. It will depend on when the contract is approved by the BPW and other factors and the target date will be agreed upon with the awarded firm. (b) The RFP references NIST SP 800-171 and CMMC as applicable compliance frameworks but does not separately identify a specific CUI environment or define a separate in-scope monitoring population for CUI-containing systems.
67	Are student and Corporate users within the same Microsoft Tenant?	Yes, different domains, but same tenant.

Question Number	Question Text	Response / Answer
68	Please confirm the number of identities in scope for monitoring. Does the scope include the full student population (in EntraID) or is it limited to faculty, staff, contractors, and privileged accounts? If student accounts are in scope, should pricing be based on total provisioned accounts, accounts active within a given term, or licensed accounts?	Offerors should use 150,000 monitored users as the planning assumption. Students are included.
69	Please provide approximate counts of in-scope managed workstations, servers, and network devices (endpoints) for staff.	Offerors should assume 4,100 endpoints/servers and 150,000 monitored users. These numbers are not expected to change significantly during the term.
70	Please clarify the expected scope of Contractor activity within the University's existing SIEM. Is the Contractor responsible for detection engineering, use case development, and maintenance of the UMGC SIEM Detection Catalog within the platform, or is the Contractor's role limited to consuming and triaging alerts generated by the platform?	The Contractor's role is broader than alert triage alone. The RFP requires optimization and definition of use cases and policies within the existing SIEM, maintenance of the UMGC SIEM Detection Catalog, documentation of newly developed or enhanced detection rules/correlation logic, and quarterly recommendations for tuning and optimization.
71	Will participation by a value-added reseller or distributor count toward the three percent MBE subc	The University does not have a preferred reseller, distributor, channel partner, or contract vehicle for this solicitation. Offerors may propose their preferred teaming arrangement, reseller, or authorized channel partner, provided the proposal clearly identifies all parties and the contractual relationship among them. Any proposed arrangement must comply with the requirements of the solicitation. If the successful Offeror intends to provide services through a reseller or channel partner, the proposal should clearly identify the role of each entity and any applicable authorizations or certifications. The MBE goal may only be satisified by working with a Certified Maryland Minority Business Enterprise (MBE) to meet the subcontracting goal. Please contact the UMGC MBE Liaison - Pamela Welzenbach - pamela.welzenbach@umgc.edu - if you have questions about the MBE forms or how to find a Certified Maryland MBE.
72	The Price Form requires a single fixed monthly amount across the three-year base term. Will UMGC permit pricing structured in tiers or bands tied to monitored endpoint or identity volume, or include an equitable adjustment mechanism if in-scope volumes change materially during the term? Relatedly, may offerors propose differentiated annual pricing within the base term?	Offerors should submit pricing in the format provided in the Price Form. The managed SOC services pricing for the base term should be proposed as fixed pricing as requested, with any relevant volume, endpoint, identity, log, or other scope assumptions clearly identified in the Price Proposal Narrative. Any additional or non-routine services should be addressed consistent with the RFP's as-needed services and rate card requirements.

Question Number	Question Text	Response / Answer
73	Does the State require any mandatory onsite staffing, or is a remote or hybrid delivery model acceptable?	All staffing would be remote. There is no expectation for onsite presence.
74	Are background checks required for all Vendor personnel, or only for personnel with physical or logical access to State systems or data?	The RFP does not expressly state background check requirements for vendor personnel. UMGC expects offerors to follow appropriate personnel screening and security practices. Any applicable personnel access requirements will be addressed in the resulting contract.
75	Please confirm whether funding for this procurement has been approved.	UMGC has authority to conduct this procurement and intends to proceed in accordance with the RFP. As stated in the solicitation, any resulting award and contract execution remain subject to the applicable approval process, including BPW approval.
76	Does the State have an estimated or not-to-exceed total contract value for the initial term and any renewal options?	No.
77	Does the State have an estimated annual contract value or anticipated annual spend associated with this procurement?	No.
78	Is there a minimum spend or volume commitment associated with this contract, or will usage be at the discretion of the State and participating agencies?	This question is not applicable to UMGC's RFP.
79	Does the State have a preferred solution, platform, or technology stack in mind for this procurement, or is the State open to alternative approaches that meet the requirements?	UMGC does not prescribe a single required solution stack beyond the solicitation requirements. Its stated preference is to use existing UMGC platforms, but alternative or complementary approaches may be proposed if they meet the requirements and are clearly explained.
80	Will the State consider vendor-proposed solutions or architectures that differ from the examples described in the RFP, provided all functional and technical requirements are met?	This question is not applicable to UMGC's RFP.
81	Please identify the incumbent vendor(s) currently providing services similar to those described in this RFP. Please provide the expiration date(s) of the incumbent contract(s), if applicable. Is the scope described in this RFP substantially similar to the incumbent scope, or does this procurement represent a material change or expansion in services?	See Response to Question No. 2 above.
82	Does the State anticipate conducting a Best and Final Offer (BAFO) phase?	UMGC may, in its sole discretion, request Best and Final Price Proposals (BAFO). A BAFO phase is therefore possible, but not guaranteed.
83	Will post-submission discussions be limited to proposal clarifications, or may limited negotiations occur prior to award?	Post-submission discussions may include clarifications and discussion of proposal content, and UMGC also reserves the right to negotiate contract terms and conditions prior to award. UMGC may make award with or without discussions or negotiation.

Question Number	Question Text	Response / Answer
84	Please provide your current daily/monthly log ingestion volume in GB.	UMGC has identified approximate SIEM ingestion of 115 GB per day. Based on that figure, monthly ingestion would be roughly 3.5 TB in a 30-day month, subject to normal fluctuation.
85	What is the expected YoY growth in log ingestion over the next 3 years?	We expect YoY growth to be about 20% after initial implementation.
86	Please provide the anticipated number and complexity of new log sources per month or year.	We anticipate 100 new log sources for the first year and then incremental after that. We do not anticipate any to be overly complex or highly customized.
87	Please share the volumes and types of log sources currently integrated with SIEM (eg, servers, endpoints, network devices, cloud platforms, cloud workloads, security tools and applications).	UMGC has identified approximately 235 currently onboarded log sources and approximate SIEM ingestion of 115 GB/day. UMGC is not providing a detailed count by source type at this time.
88	Please share the existing SIEM and SOAR platforms.	See Response to Question No 65.
89	What is the ITSM tool used by UMGC?	We use ServiceNow and much of the Azure tool suite.
90	Please provide at least the previous six months of monthly alert and incident volumes, broken down by severity, source, use case, and average handling effort.	UMGC is not providing this information at this time.
91	Please specify: i) Minimum number of proactive threat hunts expected per month or quarter ii) Whether hunts are expected to be IOC-led, hypothesis-led, or incident-led	UMGC does not prescribe a minimum number of hunts or a required monthly/quarterly cadence. Offerors should propose the frequency and methodology they believe are appropriate to meet the objectives of the solicitation.
92	Please specify whether UMGC : i) Requires an annual incident-response retainer (IRR) and, if so, the expected included hours (40 Hours/100 Hours). ii) Advanced incident response and surge support should be priced solely through the As-Needed Services rate card.	The RFP does not require a separate annual incident-response retainer or specify included annual IR hours. Offerors should clearly identify what incident response activities are included in the monthly managed SOC fee, any annual included hours if proposed, and which advanced incident response, surge, or specialized services would be priced through the As-Needed Services rate card.
93	Please specify the expected number of new or materially enhanced detection use cases, correlation rules, and automation playbooks to be delivered per month, quarter, or year.	UMGC does not specify a required numeric target for new or materially enhanced detection use cases, correlation rules, or automation playbooks by month, quarter, or year. Instead, we require ongoing development, tuning, maintenance, documentation, and quarterly recommendations for optimization and continuous improvement.

Question Number	Question Text	Response / Answer
94	Are you looking for MSSP to provide Red Team/Purple Team services?	Red Team or Purple Team services are not expressly identified as part of the routine managed SOC scope in the RFP. If UMGC elects to request additional cybersecurity services beyond the routine SOC services, such work may be obtained as As-Needed Services subject to mutually agreed work assignments and contract rates.
95	Please confirm whether UMGC permits the 24x7 SOC service to be provided through a logically segregated shared SOC model, with a dedicated Service Operations Manager. As UMGC intends to augment its existing SOC, please confirm the SOC functions that will remain with UMGC and the level of support (L1/L2/L3) expected from the service provider.	UMGC will consider a proposed SOC operating model in which services are delivered through the Offeror's SOC, provided the model is clearly described, roles and responsibilities are defined, and all service levels and requirements are met. A dedicated Service Operations Manager is required as Key Personnel. The attached RFP assigns the MSSP responsibility for end-to-end SOC services, while UMGC retains responsibilities for providing access, information, timely decisions/approvals, and stakeholder engagement. The RFP does not prescribe a fixed L1/L2/L3 allocation and expects Offerors to describe their operating model.
96	Service-credit cap: Is the 15 percent cap in Attachment B, Section 5.1 calculated against the recurring monthly Managed SOC Services fee only, or against total monthly charges including As-Needed Services?	UMGC has not designated specific Service Levels as Critical Service Levels. Offerors are expected to propose an appropriate Service Level framework, including identification of any Service Levels they consider critical and any associated service credit methodology, subject to UMGC review and acceptance. The 15% cap is an example of the kind of methodology. It's not a requirement.
97	May the proposed Service Operations Manager be an employee of a disclosed subcontractor rather than the prime Offeror?	Yes.
98	Section III, Article 1, D.7.2 requires the length of time with the Offeror but states no threshold. Is there a minimum tenure requirement, and how should this field be completed for a subcontractor employee?	No. If the Offeror is proposing a Key Personnel through a subcontractor, the Offeror must provide the length of time that personnel has worked for the subcontractor.

Question Number	Question Text	Response / Answer
99	For the monthly security and compliance reporting required for contractor- and subcontractor-owned devices used to access UMGC systems, please provide the applicable control baseline and the required report template or minimum reporting fields and supporting evidence.	For each applicable contractor device, the monthly report must include, at a minimum, the following control areas and associated details: •Antivirus – Protection status, malware detections, alerts, and reporting health. •Firewall – Firewall enabled status and policy compliance. •Patch Management – Operating system and application patch compliance, including missing critical updates. •Encryption – Full disk encryption status and any compliance exceptions. •DLP (Data Loss Prevention) – DLP compliance status and violations. •CASB Alerts – Cloud Access Security Broker alerts, including risky behavior, policy violations, data exfiltration attempts, and web security violations. •Local Administrative Privileges – Whether the contractor has local administrator access and associated approvals. •Other Security Violations – Unauthorized software installation, disabled security controls, configuration failures, peripheral device violations, and other policy violations. There is no required format for the report.
100	Section III, Article 1, D.1 requires at least one case study to include a new SOC implementation. Does onboarding a new customer onto the Offeror's existing SOC count as a "new SOC implementation," or must the case study describe building and standing up a new SOC capability?	UMGC's intent is that at least one case study demonstrate the Offeror's experience implementing SOC services for a new customer environment. This may include onboarding a new customer into the Offeror's existing managed SOC, provided the case study clearly describes the implementation effort and is comparable to the services sought in the RFP. UMGC is not requiring that the case study be limited to building a wholly new SOC capability from the ground up.
101	Section II.7 excludes subcontractor and third-party experience when determining whether the Offeror meets minimum qualifications, while Section III, Article 1, D.1.1.8 asks Offerors to identify services delivered through subcontractors or third parties. Will a case study satisfy Section II.7.3 where the Offeror was the contracting party but subcontractors or technology partners delivered part of the services?	Yes. The RFP expressly asks Offerors to identify whether services in a case study were delivered directly by the Offeror or through subcontractors, technology partners, managed service providers, or other third parties, and to describe the Offeror's role. Such case studies may be submitted, but subcontractor or third-party experience will not be used to satisfy the Offeror's separate minimum qualification requirements.
102	For the ISO/IEC 27001 alternative in Section II.7.1 and Appendix A-1, must the Offeror's certificate scope specifically include the managed SOC services proposed under this solicitation?	Yes.

Question Number	Question Text	Response / Answer
103	Must each of the three references requested in Appendix A-5 describe managed SOC services performed by the Offeror, or may references cover other comparable cybersecurity engagements?	Offerors should provide references for engagements that are comparable to the proposed services and demonstrate the Offeror's ability to perform the scope contemplated by this solicitation.
104	How will As-Needed Services rate-card pricing be incorporated into the price evaluation? Will UMGC apply assumed hours by labor category or another weighting or estimation method, and will that evaluation basis be provided to offerors?	Price Proposals will be evaluated based on overall cost, reasonableness, competitiveness, completeness, and any assumptions or risks affecting total cost of ownership.
105	While the RFP identifies evaluation criteria in descending order of importance and states that technical merit carries greater weight than price, could UMGC share the relative evaluation weights or scoring methodology to help Offerors align their proposals with the University's priorities?	UMGC does not disclose numeric weights or a more detailed scoring formula.
106	Could UMGC please clarify the requirements for the 3% MBE subcontracting goal, including whether the 3% is calculated against the initial three-year contract value or the full anticipated five-year contract value inclusive of renewal options; whether specific Maryland-certified MBE subcontractors, their scope, and participation percentages must be identified and finalized at proposal submission or may be finalized after selection/award but before contract execution; and whether MBE participation may be fulfilled through eligible supporting services such as program management, reporting, governance, or other subcontracted activities rather than direct SOC monitoring and incident response functions?	The MBE subcontracting goal is three percent (3%) of the total overall contract value, including renewal option terms, if any. Offerors must complete and submit the MBE Utilization and Fair Solicitation Affidavit & MBE Participation Schedule Form (Attachment D-1A) with the Technical Proposal. MBE participation must be performed by a Certified Maryland MBE subcontractor and may be applied to eligible subcontracted work within the scope of the contract; the attached RFP does not limit MBE participation solely to direct SOC monitoring or incident response functions.
107	Beyond the reporting requirements defined in the RFP, are there any audit support, evidence collection, control validation, or compliance reporting activities that the selected provider will be expected to perform in support of UMGC's regulatory and compliance obligations?	The selected provider is expected to align services with applicable regulatory/security frameworks and provide the required operational, incident, management, and executive reporting.
108	Are there any planned cloud migrations, infrastructure transformations, or security tool replacements anticipated during the first contract year that may impact implementation or operational support activities?	There are no planned cloud migrations, infrastructure transformations, or secuity tool replacements.
109	Has UMGC previously conducted a SOC maturity assessment or similar evaluation? If so, could the current maturity level and key improvement priorities be shared?	No, UMGC has not conduted a SOC maturity assessment.
110	The RFP specifies a False Positive Rate target of less than 10%. Could UMGC clarify whether this target is expected to be achieved immediately upon service commencement or following an agreed stabilization and optimization period during which detection rules, use cases, and monitoring content may be tuned and optimized?	We anticipate this being achieved following an agreed upon stabilization and optimization period.

Question Number	Question Text	Response / Answer
111	Does UMGC have a preference for U.S.-based, nearshore, or offshore SOC analysts supporting the 24x7 operations? Are there any restrictions regarding offshore personnel accessing UMGC systems or security data?	The Offeror must certify that it is not engaging in investment activities in Iran as described in State Finance & Procurement Article, Section 17-702, Annotated Code of Maryland. Any personnel providing services under the Contract must work from secured and compliant equipment supplied by the Offeror (or the subcontractor). The awarded Contractor will be expected to provide security and compliance reporting on a monthly basis for all resources.
112	Is prior higher education or university-sector SOC experience considered a mandatory requirement, a preferred qualification, or simply one factor in the evaluation process?	Prior higher education SOC experience is not a mandatory requirement.
113	Which SOC telemetry, incident evidence, tickets, and reports will UMGC classify as High Risk Data or CUI? Must these remain entirely within UMGC-controlled systems, or may approved contractor systems process them? Please identify the required DPA arrangements, data-location restrictions, and FIPS-validation evidence for the proposed data flows.	UMGC will provide data classification methodology, configurations and policy with the selected vendor. These will remain within the UMGC controlled systems.
114	Is there a preference to use UMGC's internal ticketing system, chat channels, and have named individuals operating in your environment for day to day activities via VDI?	Yes this is the preference.
115	Will Maryland business registration is required?	Yes, the awarded firm must be registered by time of award.
116	Do you have any ITAR/no foreign requirements? If so, do you have a separate environment for that data?	Currently we do not have any ITAR data.
117	Question1: What is the expected transition period from contract award to full operational service? Questions 2: Will UMGC provide existing runbooks, alert use cases, historical logs, architecture documentation, and current incident response procedures? Question 3: What minimum staffing and team structure required other then Service Operations Manager?	UMGC encourages Offerors to describe their approach and explain how their solution addresses the requirements in the RFP. UMGC will provide existing run books to the awarded firm.
118	Is there a need for data to stay in the US soil... also [does] the data [have] to be segregated and stored in its own instance[?]	Yes to both.