RFP# 931036 - CYBERSECURITY QUESTIONS & ANSWERS		
	QUESTIONS	**ANSWERS**
01	**Can MSU provide approximate counts or ranges of in-scope assets across each facility, including IT assets (e.g., servers, workstations, network devices), OT/SCADA devices (e.g., PLCs, HMIs, historians), user endpoints, networks (both logical and hardware diagrams), and related infrastructure, including all wireless access points, active and inactive IPs addresses that are in-scope, databases, sufficient to support scoping and pricing of the engagement, and the number of facilities or sites included in scope, sufficient to support scoping and pricing of the engagement?**	MSU will provide **available asset inventory information and approximate counts or ranges** of in-scope assets across each facility to support scoping and pricing of the engagement. This information may include, where available: 1. IT assets (e.g., servers, workstations, network devices such as firewalls, routers, and switches) 2. OT/SCADA assets (e.g., PLCs, HMIs, historians, and field devices) 3. User endpoints and supporting infrastructure 4. Network information, including logical and physical network representations 5. Wireless infrastructure components (e.g., access points) 6. IP address ranges (including active and inactive addresses), where documented 7. Databases and related application infrastructure 8. The number of facilities or sites included in scope MSU will provide this information at a level **sufficient to support high-level scoping and pricing**, typically in the form of **aggregated counts, ranges, or estimates rather than fully reconciled inventories** However: 1. The data provided may **not be exhaustive, fully normalized, or uniformly detailed across all environments** 2. Documentation completeness and granularity may vary, particularly across OT environments Accordingly, suppliers should plan to: 1. Use provided information for **initial estimation and planning purposes** 2. **Validate and refine asset counts and inventories** during the assessment 3. Identify and reconcile any gaps or discrepancies as part of their engagement approach 4. Suppliers should not assume that pre-existing documentation alone will be sufficient for detailed execution without further validation.
02	**Can MSU provide details on the types and characteristics of in-scope assets, including operating systems and versions, application types (e.g., enterprise, web, service interfaces), database technologies, whether applications are internal or internet-facing, and any relevant accessibility or architectural characteristics of these systems across IT and OT environments?**	MSU can provide general information on operating system types and environments, including: 1. IT Systems 2. Predominantly Windows-based server environments (e.g., Windows Server platforms) 3. End-user systems including Windows and macOS 4. Virtualized infrastructure platforms (e.g., hypervisor-based environments) 5. **OT / SCADA Systems** 6. Windows-based HMI, engineering workstations, and SCADA servers 7. Vendor-specific embedded or firmware-based operating systems for PLCs/RTUs 8. Mixed legacy and modern OS environments depending on facility and system lifecycle
03	**Can MSU clarify the logical and architectural structure of the in-scope environment, including the number and types of networks, segmentation between IT and OT systems, inclusion of cloud or SaaS platforms, and any boundaries, exclusions, or interconnected systems that define the assessment scope?**	MSU will provide available high-level architectural and network documentation; however, suppliers should not assume completeness and should plan to validate and refine the logical structure, segmentation, and system boundaries as part of the assessment, including IT, OT, and supporting interconnected systems.

	QUESTIONS	ANSWERS
04	**What existing documentation and artifacts will MSU provide to support the engagement, including asset inventories, network and data flow diagrams, configurations (e.g., firewall rules, remote access architecture), policies, procedures, and prior assessment reports, and to what extent are these materials expected to be complete, current, and usable for planning and execution, including whether the supplier should assume these materials will be sufficient or plan to develop and validate them during the assessment?**	Michigan State University (MSU) will provide available existing documentation and artifacts to support the planning and execution of the engagement. These materials are intended to accelerate onboarding and inform initial scoping and may include, where available: 1. Asset inventories and/or estimated counts of in-scope IT and OT assets (e.g., servers, workstations, network devices, PLCs, HMIs, historians, and field devices), sufficient to support high-level scoping and pricing 2. Network and architecture documentation, including logical and physical network diagrams and segmentation approaches 3. Available data flow or system interaction diagrams, where documented 4. Selected configuration artifacts (e.g., firewall rules, remote access architecture, VPN/jump host design), subject to security and access constraints 5. Applicable cybersecurity policies, standards, and procedures (e.g., access control, incident response, change management) 6. Relevant prior assessment reports and supporting materials (e.g., CIS-based assessments and third-party cybersecurity reviews) 7. Documentation provided by MSU should be considered directionally accurate but variable in completeness, level of detail, and currency, particularly across operational technology (OT) environments. Suppliers **should not assume that provided materials will be complete or fully current.** The selected supplier is expected to: 1. Validate and reconcile all provided documentation against the current operational environment 2. Identify gaps, inconsistencies, and outdated information 3. Develop, update, or refine asset inventories, network diagrams, and data flow documentation as needed to support the assessment 4. Collaborate with MSU stakeholders to confirm accuracy and completeness Accordingly, suppliers should plan to incorporate documentation validation and augmentation activities as part of their assessment approach and should not rely solely on existing materials for execution.
05	**Are remote access pathways, vendor-managed systems, and external or third-party access mechanisms (e.g., VPNs, jump hosts, vendor portals, cellular or dial-up access, and contractor accounts) included in scope, and if so: (a) which types of access are included; (b) how many distinct mechanisms or solutions are in scope; and (c) whether these should be evaluated for configuration, identity and access controls (including MFA), and overall security posture?**	All remote and third-party access pathways are in scope; however, suppliers should assume that inventories and documentation may be incomplete and should plan to identify, validate, and comprehensively assess these mechanisms, including configuration, access controls, MFA, and overall security posture.
06	**Can MSU confirm whether complete and current asset inventories exist for the in-scope IT and OT environments, and whether the selected supplier should plan to validate existing inventories or develop them where gaps, inaccuracies, or missing documentation are identified?**	MSU maintains asset inventories for in-scope IT and OT environments; however, **these inventories should not be assumed to be complete, fully current, or uniformly detailed across all facilities and systems**. MSU will provide available inventory data and supporting documentation to assist with initial scoping and planning, including asset counts and classifications where available. In many cases, these inventories are maintained at an aggregate or estimated level sufficient for scoping purposes rather than as fully reconciled, real-time inventories Consistent with prior assessment observations, asset inventory accuracy and completeness may vary—particularly within OT environments where **documentation is often point-in-time and subject to change** Accordingly, the selected supplier is expected to: 1. Validate and reconcile existing asset inventories against the current operational environment 2. **Identify gaps, inaccuracies, and missing assets** 3. **Augment or develop inventories** where documentation is incomplete or outdated 4. Suppliers should plan to include asset discovery, validation, and normalization activities as part of their assessment approach and should not rely solely on existing inventories for execution.
07	**Can MSU clarify any specialized or detailed inventory and assessment elements in scope beyond core assets, including firewall policies, procedural or administrative controls, supporting IT infrastructure components (e.g., jump boxes, segmentation devices), and whether detailed configuration review of OT systems (e.g., PLCs, RTUs, HMIs) is required?**	The scope includes a detailed assessment of network security controls, supporting infrastructure, administrative processes, and OT system configurations. Suppliers should plan for a comprehensive evaluation of both technical and procedural controls, including configuration review of key OT assets, where feasible and appropriate.
08	**Is wireless networking infrastructure included in scope, and if so, how many locations or environments are included and what types of wireless architectures (e.g., controller-based or access point-based) are deployed?**	Wireless infrastructure is in scope where present; however, suppliers should not assume complete inventories or uniform architectures and should plan to identify, validate, and assess wireless deployments, including architecture, configuration, and security controls, as part of the engagement.

	QUESTIONS	ANSWERS
09	**Can MSU confirm which cybersecurity frameworks and standards (e.g., NIST CSF, NIST SP 800-53, NIST SP 800-82, ISA/IEC 62443) will serve as the basis for the assessment and reporting, and whether a single primary framework should be used or a combined or multi-framework approach is expected?**	MSU expects a multi-framework approach, with a primary framework (e.g., NIST CSF or IEC 62443) supported by complementary standards such as CIS Controls and NIST SP 800-82, to ensure comprehensive coverage of both IT and OT environments.
10	**Has MSU adopted a formal cybersecurity framework for the in-scope IT and OT environments, and are existing security policies and procedures aligned with recognized standards such as NIST CSF, NIST SP 800-53/800-82, or ISA/IEC 62443, including the maturity and recency of those policies?**	MSU aligns with recognized cybersecurity frameworks (e.g., NIST CSF, CIS Controls, and applicable NIST/OT standards); however, no single framework is uniformly mandated across all environments, and policy maturity and consistency may vary. Suppliers should assess and validate the alignment, maturity, and effectiveness of existing policies and procedures as part of the engagement.
11	**Can MSU clarify expectations for mapping assessment findings to cybersecurity frameworks, including whether findings must be aligned to a single framework or multiple frameworks, and whether crosswalk mapping between frameworks is required?**	MSU expects findings to be aligned to a primary framework while supporting a multi-framework approach. Suppliers should provide crosswalk mapping between frameworks, enabling consistent reporting, traceability, and comprehensive coverage across IT and OT cybersecurity domains.
12	**Are the in-scope facilities subject to any regulatory or industry-specific cybersecurity requirements (e.g., NERC CIP or other compliance obligations), and should these be incorporated into the assessment scope?**	MSU environments may be influenced by sector-specific cybersecurity standards (e.g., power, water, OT/ICS frameworks), but formal regulatory applicability (such as NERC CIP) is not universally defined across all systems. Suppliers should incorporate regulatory and industry standards into the assessment, identify applicable requirements, and evaluate MSU's alignment as part of the engagement.
13	**Can MSU confirm which testing methods, techniques, and tools are permitted versus prohibited within IT and OT environments, including whether activities such as passive discovery, authenticated reviews, configuration extraction, and active vulnerability scanning are allowed, and identify any systems, devices, or techniques that are explicitly restricted or off-limits?**	Michigan State University (MSU) supports a structured and risk-informed approach to cybersecurity assessments across both IT and Operational Technology (OT) environments. Due to the critical nature of OT systems supporting essential infrastructure (e.g., power plant and water treatment operations), testing activities are subject to strict controls to ensure operational safety and continuity.
14	**Can MSU clarify any operational or system-specific constraints that must be followed during testing, including restrictions related to safety-critical or sensitive systems, limitations on specific tools or techniques, and any additional approvals or controls required when interacting with these environments?**	All assessment activities must be conducted using a **non-intrusive approach**, particularly within OT and safety-critical environments.Testing must not disrupt operations or impact system availability. Active or intrusive techniques including exploitation or aggressive scanning are restricted, especially for OT systems (e.g., PLCs, SCADA, and facility controls). All tools and techniques must be reviewed and approved by MSU in advance, and activities must be coordinated with MSU personnel and follow operational and safety requirements. Vendors are expected to clearly define their methodology, including any tools and access requirements, and obtain appropriate approvals prior to execution.
15	**Can MSU confirm the expected depth and type of testing for this engagement, including whether assessment activities should be limited to documentation or architecture review, passive analysis, or extended to authenticated validation, vulnerability testing, penetration testing, and hands-on assessment of OT/ICS systems (e.g., PLCs, HMIs, historians), versus primarily governance, segmentation, and control design review?**	Michigan State University (MSU) requires all cybersecurity assessment activities to adhere to strict operational, safety, and system-specific constraints. These requirements are designed to protect critical infrastructure, ensure continuity of operations, and prevent unintended impact to sensitive IT and OT environments. penetration test would not be the best method for this enviorment.
16	**Can MSU define any operational windows, maintenance periods, blackout periods, planned outages, system availability constraints, or facility dependencies that govern when testing activities may be performed, including any restrictions that may impact scheduling or sequencing of assessment activities?**	Michigan State University (MSU) requires that all cybersecurity assessment activities be carefully scheduled and coordinated to avoid disruption to critical IT and Operational Technology (OT) services. While specific operational windows may vary by system and facility, the following constraints and expectations govern when testing activities may be performed. MSU does not operate under fixed enterprise-wide testing windows; instead, all activities must be scheduled in coordination with system owners and operational teams. MSU reserves the right to restrict, reschedule, or terminate testing activities based on operational requirements, safety considerations, or system availability.
17	**Can MSU clarify how testing activities should be executed and coordinated, including whether testing may be conducted from centralized or remote locations versus requiring on-site presence, whether access to live systems (e.g., for packet capture) will be provided, and any expectations regarding sampling approaches, development of rules of engagement or test plans, and inclusion of additional assessment components such as physical security reviews?**	All testing activities must be governed by a formally approved Rules of Engagement and Test Plan. MSU reserves the right to restrict system access, require on-site coordination, or prohibit specific techniques based on operational, safety, or security considerations.
18	**Does MSU have any required or preferred templates, formats, or structural expectations for deliverables such as plans, reports, executive summaries, and remediation roadmaps, including expectations for report length or format? Additionally, can MSU clarify expectations for readout or briefing deliverables, including the number, format (technical vs. executive), and intended audiences for such sessions?**	MSU does not mandate a specific report template; however, all deliverables must be structured, actionable, and suitable for both executive and technical audiences. Vendors are expected to provide layered reporting, including an executive summary, detailed technical findings, and a prioritized remediation roadmap, along with formal briefings tailored to respective stakeholder groups.

	QUESTIONS	ANSWERS
19	**Can MSU confirm expectations for presentation-based deliverables, including the number of readout or briefing sessions, the number of executive-level summaries required, whether technical and executive readouts are expected as separate or combined sessions, the intended audiences for each (e.g., engineering, IT, security, executive leadership), and the required delivery format (onsite versus virtual)?**	MSU expects vendors to provide both executive-level and technical readouts, typically as separate sessions, unless otherwise approved. Presentations must be tailored to their intended audiences and delivered in a professional format. Virtual delivery is preferred; however, vendors must be capable of supporting onsite presentations when required.
20	**Can MSU confirm expectations for the content and level of detail within deliverables, including: (a) whether remediation roadmaps must include prioritization only or also implementation-level detail such as cost estimates, sequencing, and dependency analysis; (b) the required depth of standards or framework mapping (e.g., high-level mapping versus control-by-control mapping); (c) whether findings must include supporting evidence such as screenshots, configuration excerpts, or traffic samples, or if narrative documentation alone is sufficient; (d) whether supporting materials such as appendices, asset inventories, interview logs, evidence catalogs, or standards crosswalks are required; (e) whether findings must be validated with facility personnel or stakeholders prior to finalization of the report; and (f) the preferred risk rating or scoring methodology (e.g., qualitative, likelihood-impact, or maturity-based models) to be applied to assessment findings?**	MSU expects deliverables to provide actionable and well-supported findings, including a prioritized remediation roadmap, appropriate supporting evidence, and alignment to recognized cybersecurity frameworks. Findings should be validated with stakeholders prior to final reporting, and vendors must apply a clear, consistent risk rating methodology that supports informed decision-making.
21	**Can MSU confirm how deliverables are expected to be structured and organized, including whether a single consolidated report and remediation roadmap is preferred or separate facility-specific reports and/or roadmaps are required, whether a formal, standalone remediation roadmap must be provided, whether multiple assessments or assessment cycles are expected, how findings should be organized (e.g., by facility, control domain, system type, or risk priority), and whether the assessment should be presented using a formal maturity model or control-by-control scoring approach or as a technical risk and gap assessment with prioritized findings and recommendations?**	MSU expects a consolidated assessment report supported by structured facility-level detail and a formal remediation roadmap. Findings should be organized by risk and relevant logical groupings, and presented primarily as a risk-based assessment with actionable recommendations. Supplemental maturity or control-based scoring may be included where appropriate but should not replace clear, prioritized findings.
22	**Can MSU confirm reporting cadence and review expectations for the engagement, including: (a) whether interim deliverables (e.g., progress updates, preliminary findings, or draft reports) are required; (b) the expected frequency of status or progress reporting; and (c) the expected sequence and timing of draft versus final deliverables and any associated review cycles?**	MSU expects a structured and iterative reporting process, including regular status updates, interim or preliminary findings, and at least one formal draft review cycle prior to final deliverable submission. Vendors must proactively communicate progress and risks throughout the engagement and support collaborative review with MSU stakeholders.
23	**Can MSU confirm whether the scope of this engagement is limited to cybersecurity assessment and remediation roadmap development, or if additional post-assessment or follow-on services are expected or should be proposed, including: (a) remediation validation or retesting; (b) remediation implementation support or hands-on assistance; (c) advisory or program support services; (d) development of policies, procedures, or architectures; and (e) whether such services should be included in the base scope or proposed as optional components?**	MSU's intent for this engagement is to focus on cybersecurity assessment and remediation planning. Vendors may propose additional post-assessment services, such as remediation validation, implementation support, or program development, as optional components. These services must be clearly identified, separately scoped, and priced outside of the base engagement.
24	**Can MSU provide details on the identity and access management architecture supporting IT and OT environments, including identity sources (e.g., Active Directory, local accounts, vendor-managed identities), deployment models (on-premises, cloud, or hybrid), and the systems and assets that fall within scope for identity and access review?**	MSU operates a hybrid identity environment spanning enterprise Active Directory, cloud-based identity services, and distributed OT identity mechanisms. Vendors are expected to validate identity sources during the assessment and identify gaps in identity governance, access control, and integration across IT and OT environments.
25	**Can MSU provide information on the user population within the identity environment, including the number of users and the types of user groups (e.g., operators, engineers, IT administrators, and third-party vendors) whose access should be reviewed?**	MSU does not maintain a fully centralized inventory of all users across IT and OT environments. Vendors are expected to identify and classify user populations as part of the assessment, including administrative users, operators, engineers, service accounts, and third-party/vendor access, and to evaluate access controls and governance across all in-scope systems.
26	**Will MSU provide access to identity systems and supporting tools for the assessment, including Active Directory, identity sources, group policies, privileged account data, and any relevant monitoring or logging systems associated with identity and access management, and if so, what level of access (e.g., read-only, escorted) will be granted?**	MSU will provide access to identity systems and related data on a limited, need-to-know basis, with read-only access as the default. Access to sensitive systems, particularly within OT environments, may be restricted or require escorted or facilitated access. Vendors must clearly define their access requirements and be prepared to operate within a controlled and least-privilege access model.
27	**What level of depth does MSU expect for the identity, authentication, and authorization review, including whether the assessment should focus on architecture and process design only or include detailed validation and sampling of privileged accounts, shared accounts, local accounts, and vendor access paths?**	MSU expects the identity and access assessment to include both architectural review and targeted validation activities. Vendors must assess not only the design of identity and access controls, but also their practical implementation through sampling of privileged accounts, shared accounts, local accounts, and third-party access. A purely theoretical or architecture-only assessment will not meet MSU expectations

	QUESTIONS	ANSWERS
28	**Can MSU confirm expectations for how the engagement will be performed, including whether work should be conducted onsite, remotely, or through a hybrid model, the number and duration of any required site visits, and any expectations for onsite participation during key activities such as kickoff meetings, assessments, or reviews?**	MSU expects a hybrid delivery model, with the majority of assessment activities conducted remotely and onsite engagement utilized as needed for facility-specific activities, OT system review, and stakeholder engagement. Vendors must propose and justify any required onsite presence, including the number and duration of site visits.
29	**Can MSU confirm expectations for how the engagement should be structured and executed, including whether assessment activities should be performed sequentially or in parallel across facilities, and whether MSU prefers a defined project phase structure or expects respondents to propose their own approach?**	MSU expects vendors to propose a structured, phased approach to the assessment. While sequential coordination is expected for key planning activities, parallel execution across facilities is encouraged where appropriate. Vendors must clearly describe their methodology, including how work will be sequenced or parallelized, and how consistency and coordination will be maintained across multiple environments.
30	**Can MSU clarify expectations regarding the scope of assessment activities, including whether specific areas such as incident response capabilities, benchmarking, wireless or OT-specific environments, or implementation-level remediation planning should be included as part of the engagement?**	MSU expects the assessment to focus on core cybersecurity evaluation of IT and OT environments and development of a remediation roadmap. High-level reviews of areas such as incident response, wireless infrastructure, and framework alignment are expected where relevant. More advanced activities, including detailed benchmarking, incident response testing, or implementation support, may be proposed as optional services but are not required as part of the base scope.
31	**For the RFP's Minimum Mandatory Requirements, including cybersecurity assessment experience, OT/ICS expertise, and required certifications, how should respondents demonstrate compliance, and do these requirements apply solely to the prime contractor or may subcontractor experience be combined to meet them? Additionally, what specific qualifications, certifications, or domain experience are required or preferred?**	Respondents must demonstrate compliance with minimum mandatory requirements through documented experience, project references, and qualified personnel. Experience and qualifications may be satisfied through a combination of prime contractor and subcontractor capabilities; however, respondents must clearly define roles, responsibilities, and overall accountability. MSU expects teams to include personnel with relevant cybersecurity and OT/ICS expertise supported by industry-recognized certifications.
32	**Can MSU clarify administrative and proposal-related requirements, including availability of referenced documents, proposal structure expectations, reference submission requirements, and any historical or supporting data relevant to proposal development?**	MSU does not mandate a fixed proposal template; however, respondents must submit well-structured proposals that clearly address all RFP requirements. References and supporting documentation must demonstrate relevant experience, and any assumptions made due to incomplete data must be clearly identified. MSU will provide referenced documents and clarification responses as available; however, respondents are expected to propose solutions based on reasonable assumptions where necessary.
33	**Can MSU provide specific details about the in-scope environment, including: (a) whether the facilities are interconnected or operate as separate environments; (b) approximate user populations; (c) geographic proximity of facilities; (d) key technology platforms (e.g., OEM vendors, Microsoft licensing); (e) any operational constraints such as blackout periods; and (f) any regulatory, audit, or external requirements influencing the engagement?**	MSU has provided high-level information regarding the in-scope IT and OT environment; however, detailed architectural, operational, and user population data will be confirmed during the assessment. Respondents should assume a multi-facility, hybrid IT/OT environment with varying levels of interconnectivity and operational constraints, and should plan to validate all assumptions during the engagement.
34	**Can MSU identify the governance structure and key stakeholders for this engagement, including who will serve as the primary point(s) of contact, the availability of IT, OT, engineering, and facility staff to support interviews and data collection, and how coordination of activities such as scheduling, document collection, and site access will be managed during the engagement?**	MSU will provide a coordinated governance structure including a primary point of contact and access to relevant IT, OT, engineering, and facilities personnel. Vendors must work collaboratively with MSU stakeholders to schedule activities, collect documentation, and coordinate site access. Stakeholder availability will be managed based on operational priorities, and vendors should plan for a structured and iterative engagement model.
35	**Can MSU provide information on the current state of cybersecurity practices, including prior assessments, existing policies and procedures, documentation maturity, risk management processes, and other baseline capabilities within the IT and OT environments?**	MSU has conducted targeted cybersecurity assessments within portions of its environment and maintains foundational cybersecurity practices; however, the maturity and consistency of these practices vary across systems and facilities. Respondents should expect to validate existing policies, procedures, and controls as part of the engagement and identify opportunities to establish a more consistent, enterprise-wide cybersecurity posture
36	**Can MSU confirm whether this requirement is new or currently supported by an incumbent vendor, and if so, provide details including vendor name, contract scope, contract term, and whether the incumbent is eligible to compete in this RFP?**	MSU does not identify a formal incumbent vendor for this engagement. While prior vendor engagements and assessments have occurred in portions of the environment, there is no active contract covering the full scope of this RFP. All qualified respondents, including those with prior MSU experience, are eligible to compete in accordance with procurement requirements.
37	**Can MSU clarify policies governing staffing and resource usage for this engagement, including whether subcontractors or affiliated resources may be used, whether offshore delivery is permitted and any associated data access restrictions, requirements for submitting named or sample resumes, and whether substitution of proposed personnel is allowed after proposal submission?**	Respondents may utilize subcontractors or affiliated resources; however, all personnel must be clearly identified and qualified for their assigned roles. Any offshore delivery must be disclosed and will be subject to MSU security and data access requirements. Respondents must provide named personnel for key roles along with detailed qualifications. Substitution of proposed personnel after award must be approved by MSU and require equivalent or greater qualifications.
38	**Can MSU confirm whether there are any confidentiality, export control, data classification, or sensitive infrastructure handling requirements beyond standard cybersecurity engagement protections that must be followed during this engagement?**	MSU requires vendors to adhere to strict confidentiality and data protection practices appropriate for sensitive IT and OT environments. While no additional export control requirements are explicitly defined, all data accessed during the engagement must be treated as sensitive and handled in accordance with industry-standard security practices. Vendors must ensure that all personnel, systems, and processes used to support the engagement comply with applicable security and data handling requirements.
39	**Can MSU clarify requirements and expectations for on-site access to facilities during the engagement, including safety requirements, badging, physical access procedures, provision of temporary accounts, and whether escorted access or on-site support personnel (e.g., technical liaisons) will be provided for assessment activities?**	MSU will provide controlled access to facilities as required, including badging and coordination with facility personnel. Vendors must comply with all safety and operational requirements. Access to sensitive environments, particularly OT systems, may require escorted access and support from MSU personnel. Temporary system access may be provided where necessary and will be restricted in accordance with MSU security policies.

	QUESTIONS	ANSWERS
40	**Can MSU clarify requirements for handling sensitive information during and after the engagement, including guidance for FOIA considerations, labeling or redaction of sensitive findings, and any data handling, storage, residency, or destruction requirements?**	MSU requires vendors to treat all information obtained during the engagement as confidential and sensitive. As a public institution, MSU is subject to applicable FOIA requirements; therefore, vendors must clearly identify confidential information within deliverables. Vendors must implement appropriate data handling, storage, and security controls, including restrictions on data access and residency. Upon completion of the engagement, all MSU data must be returned or securely destroyed in accordance with agreed-upon procedures.
41	**Can MSU provide details on the current monitoring and detection capabilities across IT and OT environments, including the use of SIEM platforms, intrusion detection systems, OT-specific monitoring tools, centralized logging systems, and other alerting or anomaly detection technologies?**	MSU maintains foundational monitoring and detection capabilities across its IT and OT environments; however, the level of centralization and maturity may vary across systems. Vendors are expected to assess existing capabilities, including logging, detection, and alerting mechanisms, and identify opportunities to enhance visibility, correlation, and response across both IT and OT environments.
42	**Can MSU provide information on incident response capabilities, including whether a formal incident response plan is in place and how frequently incident response procedures are tested or exercised?**	MSU maintains foundational incident response capabilities; however, the maturity, consistency, and frequency of testing may vary across IT and OT environments. Vendors are expected to evaluate existing incident response plans, processes, and testing practices, and provide recommendations to enhance incident readiness, response coordination, and alignment with industry best practices.
43	**Can MSU provide details regarding log management practices across IT and OT environments, including log retention periods, storage volumes, log availability, and the overall scale and accessibility of logging data for monitoring, detection, and investigative purposes?**	MSU has not provided enterprise-wide details on log retention periods, storage volumes, or overall logging scale in the current RFP materials. Logging and monitoring capabilities exist in portions of the environment, but may vary in centralization and maturity. Vendors should validate log availability, retention, and accessibility during discovery and assess opportunities to improve aggregation, visibility, and investigative use.
44	**Can MSU confirm whether an overall budget, estimated range, or not-to-exceed amount has been established for this engagement, and whether this information will be shared with respondents?**	MSU has not established or disclosed a budget, cost range, or not-to-exceed amount for this engagement in the current RFP materials. Budget information will not be shared with respondents. Vendors should propose pricing based on their understanding of the scope, including any assumptions.
45	**Can MSU clarify the expected pricing model and contract structure for this engagement, including whether proposals should be structured as firm fixed price, time-and-materials, not-to-exceed, or another model, and how pricing submissions will be evaluated?**	MSU does not prescribe a specific pricing model or contract structure in the current RFP materials. Respondents may propose an approach (e.g., fixed price, time-and-materials, not-to-exceed, or hybrid) that aligns with their scope. Pricing must be clear, complete, and include all assumptions. It will be evaluated based on alignment with scope, transparency, reasonableness, and overall value.
46	**Does MSU require pricing to be submitted in a specific format, such as hourly rates, or will respondents be permitted to provide alternative structures such as phase-based or deliverable-based pricing summaries?**	MSU does not prescribe a specific pricing format in the current RFP materials. Respondents may use hourly, phase-based, or deliverable-based pricing, provided it is clear, complete, and aligned to the scope.
47	**Can MSU clarify expectations regarding travel and reimbursable expenses, including whether estimated travel costs should be included in pricing submissions and whether any caps or not-to-exceed limits apply?**	MSU has not defined specific requirements for travel or reimbursable expenses in the current RFP materials. Vendors should include all travel costs in their pricing and clearly state assumptions. No caps or not-to-exceed limits are specified.
48	**Can MSU confirm the official proposal submission deadline, including resolution of any discrepancies between stated dates in the RFP and whether an addendum will be issued to clarify the timeline?**	MSU confirms that the official proposal submission deadline is as stated in the RFP. If any discrepancies exist between dates, they will be clarified through a formal addendum issued to all respondents. Any updates to the timeline will also be communicated via addendum.
49	**Can MSU confirm the anticipated project start date, including whether the stated timeline (e.g., September 2026) is a fixed start date or an estimated timeframe?**	MSU has not defined a fixed project start date within the current RFP materials. Any referenced timing (e.g., September 2026) should be considered an estimated timeframe, subject to procurement timelines, contract execution, and project coordination. The final start date will be confirmed with the selected vendor following award.
50	**Can MSU clarify expectations for project duration and completion, including whether a target end date, maximum timeframe, or preferred engagement duration has been established, or whether respondents should propose duration based on their methodology and approach?**	MSU has not established a fixed project duration, target end date, or maximum timeframe in the current RFP materials. Respondents should propose an appropriate engagement duration based on their methodology, scope, and approach, clearly outlining assumptions and key milestones.