MICHIGAN STATE UNIVERSITY

REQUEST FOR PROPOSAL
RFP# 931036

Cybersecurity Assessment

RFP Timeline	
RFP Issue Date	May 4, 2026
Deadline for Respondent Questions to MSU	May 20, 2026
MSU deadline for providing response	May 27, 2026
RFP Response Due Date	**June 3, 2026, 3:00 pm Eastern**
Estimated Contract Award	July, 2026

RFP Contact	
Name:	Keith Duckworth
Unit:	MSU Procurement
Email:	duckwo26@msu.edu
Phone:	517-884-6162

DESCRIPTION: Michigan State University (the "**University**" or "**MSU**") is soliciting proposals through this Request for Proposal ("**RFP**") for the purpose of Michigan State University ("MSU") is soliciting proposals from qualified firms to perform a **comprehensive cybersecurity assessment** of information technology (IT) and operational technology (OT) environments supporting the University's **Water Treatment Facility** and the **T.B. Simon Power Plant**.

The purpose of this RFP is to evaluate the current cybersecurity posture of these environments, identify technical vulnerabilities and control gaps, and provide risk-based, actionable recommendations that account for the operational, safety, and availability requirements of critical infrastructure systems. Services are expected to include assessment of network architecture, systems, access controls, monitoring capabilities, and alignment with applicable cybersecurity standards.

The requested services are more thoroughly described under the Scope of Work Section of this RFP. Firms intending to respond to this RFP are referred to herein as a "**Respondent**" or "**Supplier**."

MICHIGAN STATE UNIVERSITY

PROPOSAL INSTRUCTIONS

1. **PROPOSAL PREPARATION.** The University recommends reading all RFP materials prior to preparing a proposal, particularly these Proposal Instructions. Respondents must follow these Proposal Instructions and provide a complete response to the items indicated in the table below. References and links to websites or external sources may not be used in lieu of providing the information requested in the RFP within the proposal. Include the Respondent's company name in the header of all documents submitted with your proposal.

Document	Description	Response Instructions
Cover Page	Provides RFP title and number, important dates, and contact information for MSU	Informational
Proposal Instructions	Provides RFP instructions to Respondents	Informational
Respondent Information Sheet	Company and Contact Information, and Experience	Respondent must complete and submit by proposal deadline
Scope of Work	Describes the intended scope of work for the RFP	Respondent must complete and submit by proposal deadline
Pricing	Pricing for goods and services sought by the University through this RFP	Respondent must complete and submit by proposal deadline
Master Service Agreement	Provides legal terms for a contract awarded through this RFP	Deemed accepted by Respondent unless information required in **Section 9, Master Service Agreement** is submitted by proposal deadline

2. **EXPECTED RFP TIMELINE**.

Activity	Date
Issue RFP	May 4, 2026
Deadline for Respondent Questions to MSU	May 20, 2026
RFP Response Due	**June 3, 2026, 3:00 pm Eastern**
Estimated Contract Award	July, 2026

3. **CONTACT INFORMATION FOR THE UNIVERSITY.** The sole point of contact for the University concerning this RFP is listed on the Cover Page. Contacting any other University personnel, agent, consultant, or representative about this RFP may result in Respondent disqualification.

4. **QUESTIONS.** Respondent questions about this RFP must be submitted electronically by email to the contact listed on the cover page of this RFP. In the interest of transparency, only written questions are accepted. Answers to all questions will be sent to Respondents via email. Submit questions by referencing the following: (i) Question Number, (ii) Document Name, (iii) Page Number, and (iv) Respondent Question. Please refer to **Section 2** above for the deadline to submit questions.

5. **MODIFICATIONS.** The University may modify this RFP at any time. Modifications will be sent via email. This is the only method by which the RFP may be modified.

6. **DELIVERY OF PROPOSAL.** The Respondent must submit its proposal, all attachments, and any modifications or withdrawals electronically via email to the contact listed on the cover page of this RFP. **The price proposal should be saved separately from all other proposal documents and should be sent as a separate attachment from the other proposal documents.** The Respondent should submit all documents in a modifiable (native) format (examples include but are not limited to: Microsoft Word or Excel and Google Docs or Sheets). In addition to submitting documents in a modifiable format, the Respondent may also submit copies of documents in PDF. Respondent's failure to submit a proposal as required may result in disqualification. The proposal and attachments must be fully uploaded and submitted prior to the proposal deadline. **Do not wait until the last minute to submit a proposal**. The University **may not** allow a proposal to be submitted after the proposal deadline identified in the Cover Page, even if a portion of the proposal was already submitted.

7. **MANDATORY MINIMUM REQUIREMENTS.** The RFP may contain minimum qualifications, which will be identified as "**Mandatory Minimum Requirements**" in the Scope of Work Section of this RFP. If the RFP does contain mandatory minimum requirements, any proposal not meeting these minimum requirements **will be deemed non-qualified and will not be considered**. All proposals meeting these mandatory minimum requirements will proceed for review and evaluation consistent with **Section 8**, **Evaluation Process**.

8. **EVALUATION PROCESS.** The University will convene a team of individuals from various Departments within MSU to evaluate each proposal based on each Respondent's ability to provide the required services, taking into consideration the overall cost to the University. The University may require an oral presentation of the Respondent's proposal; conduct interviews, research, reference checks, and background checks; and request additional price concessions at any point during the evaluation process. The following criteria will be used to evaluate each proposal:

Criteria	Weight
Implementation Strategy (approach to the scope of work), methodology and Project plan	40%
Relevant Experience and Qualifications	30%
Price	20%
Supplier Risk and Compliance (Adherence to legal terms, etc.)	10%
	100%

9. **MASTER SERVICE AGREEMENT**. The University strongly encourages strict adherence to the terms and conditions set forth in the Master Service Agreement. The University reserves the right to deem a proposal non-responsive for failure to accept the Master Service Agreement. Nevertheless, the Respondent may submit proposed changes to the Master Service Agreement in track changes (i.e., visible edits) with an explanation of the Respondent's need for each proposed change. Failure to include track changes with an explanation of the Respondent's need for the proposed change constitutes the Respondent's acceptance of the Master Service Agreement. General statements, such as "the Respondent reserves the right to negotiate the terms and conditions," may be considered non-responsive.

10. **CLARIFICATION REQUEST.** The University reserves the right to issue a Clarification Request to a Respondent to clarify its proposal if the University determines the proposal is not clear. Failure to respond to a Clarification Request timely may be cause for disqualification.

11. **RESERVATIONS.** The University reserves the right to:
    a. Disqualify a Respondent for failure to follow these instructions.
    b. Discontinue the RFP process at any time for any or no reason. The issuance of an RFP, your preparation and submission of a proposal, and the University's subsequent receipt and evaluation of your proposal does not commit the University to award a contract to you or anyone, even if all the requirements in the RFP are met.
    c. Consider late proposals if: (i) no other proposals are received; (ii) no complete proposals are received; (iii) the University received complete proposals, but the proposals did not meet mandatory minimum requirements or technical criteria; or (iv) the award process fails to result in an award.
    d. Consider an otherwise disqualified proposal, if no other proposals are received.
    e. Disqualify a proposal based on: (i) information provided by the Respondent in response to this RFP; or (ii) if it is determined that a Respondent purposely or willfully submitted false or misleading information in response to the RFP.
    f. Consider prior performance with the University in making its award decision.
    g. Consider total-cost-of-ownership factors (e.g., transition and training costs) when evaluating proposal pricing and in the final award.
    h. Refuse to award a contract to any Respondent that has outstanding debt with the University or has a legal dispute with the University.
    i. Require all Respondents to participate in a Best and Final Offer round of the RFP.
    j. Enter into negotiations with one or more Respondents on price, terms, technical requirements, or other deliverables.
    k. Award multiple, optional-use contracts, or award by type of service or good.
    l. Evaluate the proposal outside the scope identified in **Section 8, Evaluation Process**, if the University receives only one proposal.
    m. Obtain and consider information from other sources concerning a Respondent, such as the Respondent's capability and performance under other contracts, the qualifications of any subcontractor identified in the Proposal, the Respondent's financial stability, past or pending litigation, and other publicly available information.
    n. Utilize third parties to assist in the evaluation process, provided such parties are subject to confidentiality requirements.

12. **AWARD RECOMMENDATION.** The contract will be awarded to the responsive and responsible Respondent who offers the best value to the University, as determined by the University. Best value will be determined by the Respondent meeting any mandatory minimum requirements and offering the best combination of the factors in **Section 8**, **Evaluation Process**, and price, as demonstrated by the proposal. The University will email a **Notice of Award** to all Respondents. A Notice of Award does not constitute a contract, as the parties must reach final agreement on a signed contract before any services can be provided. The awarded Respondent is prohibited from partnering with losing bidders unless the RFP specifically allows for such arrangement, and any violation of this prohibition may result in disqualification of the awarded Respondent.

13. **GENERAL CONDITIONS.** The University will not be liable for any costs, expenses, or damages incurred by a Respondent participating in this solicitation. The Respondent agrees that its proposal will be considered an offer to do business with the University in accordance with its proposal, including the Master Service Agreement, and that its proposal will be irrevocable and binding for a period of 180 calendar days from date of submission. If a contract is awarded to the Respondent, the University may, at its option, incorporate any part of the Respondent's proposal into the contract. This RFP is not an offer to enter into a contract. This RFP may not provide a complete statement of the University's needs, or contain all matters upon which agreement must be reached. Proposals submitted via email are the University's property.

14. **FREEDOM OF INFORMATION ACT.** Respondent acknowledges that any responses, materials, correspondence or documents provided to the University may be subject to the State of Michigan Freedom of Information Act ("FOIA"), Michigan Compiled Law 15.231 *et seq*., and may be released to third parties in compliance with FOIA or any other law. Questions about the Respondent's own performance can be directed to the RFP Contact indicated on page 1 of this document. Questions about the overall evaluation and any other post-award inquiries must be submitted via a formal FOIA request to the Michigan State University FOIA office.

MICHIGAN STATE UNIVERSITY

RESPONDENT INFORMATION SHEET

Please complete the following Information Sheet in the space provided:

Information Sought	Response
Contact Information	
Respondent's sole contact person during the RFP process. Include name, title, address, email, and phone number.	
Person authorized to receive and sign a resulting contract. Include name, title, address, email, and phone number.	
Respondent Background Information	
Legal business name and address. Include business entity designation, e.g., sole proprietor, Inc., LLC, or LLP.	
What state was the company formed in?	
Main phone number	
Website address	
DUNS# AND/OR CCR# (if applicable):	
Number of years in business and number of employees	
Legal business name and address of parent company, if any	
Has your company (or any affiliates) been a party to litigation against Michigan State University? If the answer is yes, then state the date of initial filing, case name and court number, and jurisdiction.	
Experience	
Describe relevant experiences from the last 5 years supporting your ability to successfully manage a contract of similar size and scope for the services described in this RFP.	
Experience 1	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 2	
Company name Contact name Contact role at time of project Contact phone	

Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 3	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	

NOTE: ***Please ensure that the people you noted as "contact" can be reached via the information provided and are aware that MSU may be reaching out during this RFP.***

MICHIGAN STATE UNIVERSITY

SCOPE OF WORK

Please address each of the sections below in a written response, which can be completed on a separate sheet (using the same section headings).

1. Background.

Cybersecurity assessments are a critical component of risk management for environments that support operational technology (OT), industrial control systems (ICS), and critical infrastructure. Water treatment and power generation facilities depend on highly available, deterministic systems that must be secured without disrupting operations or compromising safety. Threat actors increasingly target these environments due to their reliance on legacy protocols, flat network architectures, and convergence of IT and OT networks.

2. Objective

This engagement focuses on evaluating the cybersecurity posture of systems supporting the Water Treatment Facility and the T.B. Simon Power Plant. The assessment will identify technical vulnerabilities, architectural weaknesses, and control gaps across IT, OT, and hybrid environments. Results will support risk-informed decision-making, compliance alignment, and prioritization of remediation activities while accounting for operational constraints typical of industrial environments.

A. Assignment Overall Goal & Objective

The overall goal of this engagement is to perform a technically rigorous cybersecurity assessment of IT and OT systems supporting the Water Treatment Facility and the T.B. Simon Power Plant.

The objectives are to:

- Identify technical vulnerabilities, misconfigurations, and architectural weaknesses across network, system, and application layers.
- Assess cybersecurity risks to availability, integrity, and confidentiality of operational systems.
- Evaluate the effectiveness of existing technical, administrative, and procedural security controls.
- Produce a prioritized, risk-based remediation roadmap aligned with industry standards and operational realities.

B. Specific Objectives

- Assess cybersecurity risks associated with ICS, SCADA, PLCs, HMIs, historians, and supporting infrastructure.
- Evaluate IT/OT network segmentation, trust boundaries, firewall policies, and remote access mechanisms.
- Review identity, authentication, and authorization mechanisms for privileged and non-privileged access.
- Assess logging, monitoring, detection, and incident response capabilities for OT-relevant threats.
- Measure alignment with applicable standards such as NIST Cybersecurity Framework (CSF), NIST SP 800-53/82, and ISA/IEC 62443.

3. Scope of Work.

Services will include, but are not limited to, the following technical activities:

A. Planning and Initiation

- Conduct technical kickoff sessions with IT, OT, and facility stakeholders.
- Define scope boundaries, including systems in-scope, out-of-scope, and testing constraints.
- Document assumptions related to system uptime, safety, and non-intrusive testing requirements.
- Develop a detailed engagement plan, data request list, and communication protocol.

B. Asset Discovery and Architecture Review

- Validate and document inventories of IT and OT assets, including servers, network devices, field devices, and applications.
- Review logical and physical network diagrams, data flows, and trust relationships.
- Identify critical systems and single points of failure.

C. Technical Security Assessment

- Perform configuration and control reviews of firewalls, switches, routers, and network segmentation controls.
- Conduct vulnerability assessments of servers, operating systems, applications, and network devices using non-disruptive methods.
- Review secure configuration baselines, patch management practices, and hardening standards.
- Evaluate remote access solutions (VPNs, jump hosts, vendor access paths) and associated controls.

D. Identity, Access, and Privilege Review

- Assess identity sources (e.g., Active Directory, local accounts) and integration with OT systems.
- Review privileged access management, credential storage, and authentication mechanisms.
- Evaluate role-based access controls and separation of duties.

E. Monitoring, Detection, and Response

- Review logging configurations, log retention, and visibility across IT and OT environments.
- Assess intrusion detection, anomaly detection, and alerting capabilities.
- Evaluate incident response procedures specific to ICS and critical infrastructure scenarios.

F. Risk and Gap Analysis

- Identify vulnerabilities, misconfigurations, and control deficiencies.
- Analyze risk in terms of likelihood and impact to safety, operations, compliance, and reliability.
- Map findings to relevant cybersecurity frameworks and standards.

G. Reporting and Technical Readout

- Produce a comprehensive technical assessment report.
- Conduct technical readout sessions for engineering, IT, and security personnel.
- Deliver executive-level summaries for leadership.

4. EXPECTED DELIVERABLES / OUTCOMES

A. Detailed Engagement Plan and Technical Approach

B. Cybersecurity Assessment Report, including:
- System and network architecture analysis
- Assessment methodology and tools used
- Detailed findings with technical evidence
- Risk ratings and impact analysis
- Mapping to NIST CSF, NIST 800-series, and IEC 62443 controls

C. Prioritized Remediation Roadmap
- High-risk and near-term mitigation actions
- Medium- and long-term security architecture improvements

D. Actionable Technical Recommendations
- Configuration, architectural, and procedural improvements
- Consideration for operational safety and system availability

5. ASSIGNMENT DURATION

The assignment is expected to commence in September 2026, and Suppliers are expected to propose duration based on your approach and methodology. Suppliers must define discrete technical phases such as assessment, analysis, validation, and remediation planning within this timeframe.

6. IMPLEMENTATION STRATEGY AND PROJECT PLAN

Suppliers must propose a technically sound implementation strategy that reflects

Suppliers are required to propose the best implementation strategy and approach that will accomplish/address the scope of this assignment (critical infrastructure constraints.). A preliminary project plan and schedule should be in sufficient detail to clearly outline tasks and timelines for implementation of the strategies. The schedule should show the expected sequence of tasks and include proposed durations for the performance of each task. The proposed Project Plan must include:

- Defined assessment phases and milestones
- Dependencies on system availability and operational windows
- Roles and responsibilities for supplier and MSU staff

Proposals will be evaluated and scored in accordance with section 7.

7. QUALIFICATIONS AND EXPERIENCE

A. Company Qualifications and Experience

i. Industry Experience: Minimum of ten (10) years of cybersecurity consulting experience, including OT, ICS, or critical infrastructure environments.

ii. Comparable Engagements: Demonstrated experience assessing cybersecurity for organizations comparable in size and complexity to Michigan State University.
iii. Framework Alignment: Show experience performing assessments aligned with recognized cybersecurity frameworks and standards, including at a minimum NIST Cybersecurity Framework (CSF) and NIST SP 800-series (e.g., 800-53, 800-82) and/or ISA/IEC 62443.
iv. Non-Disruptive Testing: Demonstrate the ability to conduct assessments using non-intrusive and operationally safe testing methods appropriate for critical infrastructure environments.
v. Qualified Personnel: Assign personnel with documented experience in cybersecurity assessments of comparable scope and complexity, including senior technical staff with direct hands-on assessment experience.
vi. Independence and Objectivity: Disclose any current or recent engagements with MSU and demonstrate independence and absence of conflicts of interest that could affect objectivity of findings.
vii. Reporting Capability: Demonstrate the ability to deliver technically detailed assessment reports that include evidence-based findings, risk prioritization, and actionable remediation recommendations suitable for both technical and executive audiences.
viii. Methodology: Use of established, repeatable methodologies aligned with recognized cybersecurity standards.

B. Core Team Qualifications and Experience

The proposed engagement team must include a minimum of three senior-level consultants who will directly facilitate the assessment and organizational development work.

A. Technical Team Lead: The Team Leader must demonstrate possessing the following minimum qualifications
i. At least five (5) years of experience leading cybersecurity or infrastructure assessments.
ii. Demonstrated experience with OT/ICS security architecture and risk assessment.
iii. Proficiency with project management methodologies and technical reporting.
iv. Prior higher education or critical infrastructure experience.

B. Senior Consultant / Analyst I: The Sr Consultant/ Analyst I must demonstrate possessing the following minimum qualifications
i. At least three (3) years of hands-on cybersecurity assessment experience.
ii. Experience assessing networks, systems, and applications in complex environments.
iii. Familiarity with vulnerability assessment tools and cybersecurity frameworks.
iv. Strong technical documentation and stakeholder communication skills.

C. Senior Consultant / Analyst II: The Sr Consultant/ Analyst II must demonstrate possessing the following minimum qualifications
i. At least three (3) years of hands-on cybersecurity assessment experience.
ii. Experience assessing networks, systems, and applications in complex environments.
iii. Familiarity with vulnerability assessment tools and cybersecurity frameworks.
iv. Strong technical documentation and stakeholder communication skills.

The proposal must clearly define team roles and demonstrate how combined expertise supports execution of the scope.

8. MINIMUM MANDATORY REQUIREMENTS

To be considered for further evaluation, the Supplier must meet all of the following mandatory requirements:

- **A.** Demonstrated Experience: Have at least ten (10) years of experience conducting technical cybersecurity assessments for universities or organizations of comparable size and complexity to Michigan State University, including environments with distributed networks and large user populations.
- **B.** OT / ICS Expertise: Demonstrate proven experience assessing operational technology (OT) and industrial control system (ICS) environments, such as SCADA systems, PLCs, HMIs, and supporting infrastructure, in a manner that accounts for safety, availability, and operational constraints.

9. REQUIRED DOCUMENTS FOR RFP SUBMISSION

- **A.** Written response to Scope of Work
- **B.** Completed Respondent Information Sheet with the 3 required experiences.
- **C.** Implementation Strategy and Project Plan
- **D.** Other information about company required under #10 of Scope of Work Section
- **E.** Signed Pricing Proposal valid for 180-days and confirming acceptance of payment terms
- **F.** Master Service Agreement (if requesting redlines)

10. TRAVEL

- **A.** All travel and costs must be preapproved by the University
- **B.** All travel shall be reimbursed at actual cost and shall be subject to MSU's Travel Reimbursement Policy set forth at Michigan State University Office of the Controller (msu.edu)

11. INVOICING

i. Invoice Billings
   a. Each invoice is to be billed on a separate sheet of paper.
   b. Each invoice must be billed within 30 days after the completion of the stated work.
   c. All invoices are to be emailed or mailed to MSU Accounts Payable. Do not mail or email invoices to Administration Building or MSU Client, they will not be paid and will delay receipt of payment
   d. If invoices for reimbursement of travel expenses, receipts for actual travel costs shall be provided as supporting documentation along with the invoice
   e. More information on MSU invoice submission requirements can be found at: https://upl.msu.edu/finance-analytics/accounts-payable/submitting-invoices/index.html

ii. Invoice Requirements

a. Every invoice must show

(1) Company Name

(2) University Purchase Order Number

(3) Itemized/Breakdown of costs being invoiced

MICHIGAN STATE UNIVERSITY

PRICING

Please include a Pricing proposal as identified below on a separate sheet.

All pricing includes hourly rates and estimates total hours for each Team member required to work on the assignment.

The signature below confirms that this proposal is valid for 180 days after the due date.

Supplier

Signature: _____

Name: _____

Title: _____

Date: _____

MICHIGAN STATE UNIVERSITY

MASTER SERVICE AGREEMENT

(attached)

Please refer to Section 9 of the RFP Instructions when reviewing the Master Services Agreement terms and conditions.