Master Service Agreements
Statement of Work (SOW)
Service Category: Technical Analyst
Title: Cybersecurity Staff Augmentation

I. Master Service Agreements Statement of Work

Defined. The State of Minnesota, State Court Administrator's Office ("State") is using a competitive selection process (referred to herein as the "Statement of Work" or "SOW") through its Master Service Agreements program to select a vendor responsible for providing technical analysis services for various Informational Technology Division cybersecurity work efforts. This is not a bid, but a Statement of Work that could become the basis for negotiations leading to a Work Order Contract under the vendor's Master Service Contract to provide the services described herein.

Only vendors that have been selected as a Master Service Agreements vendor with the State following submission of a proposal to the Master Service Agreements for IT Technical/Infrastructure Services & IT Application/Development and Support Services Request for Proposal, and have an approved Master Service Contract with the State for the service category requested herein, may submit a response to this Statement of Work and be considered for a Work Order Contract to provide the services described herein.

Right to Cancel. The State is not obligated to respond to any proposal submitted, nor is it legally bound in any manner whatsoever by the submission of a proposal or response to this Statement of Work. The State reserves the right to cancel or withdraw this Statement of Work at any time if it is considered to be in its best interest. In the event the Statement of Work is cancelled or withdrawn for any reason, the State shall not have any liability to any proposer for the costs or expenses incurred in conjunction with this Statement of Work or otherwise. The State also reserves the right to reject any or all proposals, or parts of proposals, to waive any informalities therein, and to extend proposal due dates.

II. Business Need

The Information Technology Division (ITD) of the State Court Administrator's Office (State), located at the Minnesota Judicial Branch (MJB), is seeking one (1) Cybersecurity Analyst to support the Identity and Access Management (IAM) and Security Operations Center (SOC) teams with day-to-day operational tasks and cybersecurity projects underway at the Minnesota Judicial Branch. The list below indicates the work efforts for which the Cybersecurity Analyst would have responsibilities:

- Develop, document, maintain, and implement statewide standards to support MJB system and application IAM activities.
- Serve as the key technical resource for any IAM efforts, projects, and applications with an understanding of Multi Factor Authentication concepts and the implementation and auditing of IAM compliance.
- Troubleshoot and resolve access-related issues, specifically around identities, access, accounts, authentication, entitlements, and permissions of MJB systems and applications.

- Participate in application and network assessments to ensure appropriate IAM policies and standards are followed across MJB and mitigate any risk posed by IAM deficiencies either in the network or in applications.
- Participate with application and infrastructure architects to provide security overlays and controls for IAM development and deployment patterns.

III. Deliverables

The State IAM manager and the SOC manager will work with the contracted Cybersecurity Analyst to determine the specific and necessary deliverables for each work effort based on priority and on how each of the efforts are progressing during the contracted timeframe.

The following deliverables will be expected from the Cybersecurity Analyst. It should be noted that not all work efforts may be fully completed in the time period contracted.

- Scripting and programming
  - Perform cybersecurity programming and scripting tasks for operations and identity teams
  - Provide guidance to cybersecurity team members as a scripting and programming subject matter expert
- Access Audits
  - Perform periodic user access audits
  - Work with MJB managers on disposition of separated employee accounts
  - Streamline user access audit processes using available tools and augment with scripts
- Tool Support
  - Support maintenance, configuration and administration of MJBs Privileged Access Management solution
  - Support maintenance, configuration and administration of MJBs Identity Governance solution
  - Support maintenance, configuration and administration of MJBs Identity Provider solution including but not limited to Multifactor Authentication, Single Sign-on and Conditional access policies
  - Maintain and optimize security tools like firewalls, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions
  - Configure tools to ensure accurate logging, alerting, and detection of potential threats.
- On-call Support
  - Participate in the cybersecurity ticket support rotation as an incident responder and ticket router.
  - Provide Level 2 support for ServiceNow tickets. Support, analyze, and gather information for escalation as needed.
  - Off-hours availability not required.
- Cyber Security Operations Center Activities
  - Analyze, investigate, contain and mitigate security incidents and data breaches. Conduct root cause analysis, and determine the severity and impact of incidents
  - Monitor and analyze security alerts and events generated by various security tools
  - Ensure adherence to security policies and compliance requirements
  - Document security incidents, investigations, and responses for future reference.

- Work closely with IT teams to ensure that security controls are implemented effectively
- Collaborate on projects such as new software deployments or infrastructure changes to integrate security requirements early in the process
- Stay current on emerging threats, vulnerabilities, and security technologies
- Participate in cybersecurity training, certifications, and conferences to stay ahead in the evolving cybersecurity landscape

IV. Milestones and Schedule

Milestones and scheduled completion dates will be based upon:

- Scope for each individual work effort
- Will vary for each work effort project depending on Cybersecurity team priorities
- Will be negotiated with the IAM and SOC managers.

V. Contract Work Location and Hours

- The work locations will be at the address listed below. However, candidate may conduct work from a remote location while the Minnesota Judicial Branch continues to operate under pandemic-related workplace restrictions.

  Minnesota Judicial Center
  25 Rev. Dr. Martin Luther King Jr. Blvd,
  St. Paul, Minnesota, 55155.
- Business hours are Monday through Friday, 8:00 AM to 4:30 PM.
- The Cybersecurity Analyst is expected to work full-time hours during normal business hours unless otherwise agreed in advance with the contract manager.
- The contract timeframe has an anticipated start date of January 20, 2025. Contract will run through the end of the state fiscal year, 2025 with option to extend.

VI. Responsibilities Expected of the Selected Vendor

- The vendor must initiate and provide a criminal background check for submitted contractors.
- The vendor will provide activity plan(s) and schedule(s) agreeable to the ITD Manager.
- The vendor will assign a primary contact that will be responsible for all formal communications between the vendor and the ITD manager in regards to the contract.
- The vendor and contractor will act in a professional manner and abide by all rules set forth by the Minnesota Judicial Branch.
- The contractor will report to the ITD manager and will be expected to communicate on a regular basis (as determined by the ITD manager) with all stakeholders.
- The selected contractor will follow State disciplines standards, including use of State templates, methods and forms.

VII. Qualifications and Skills

Master Service Contract Resource Category: Technical Analyst
Resume must clearly demonstrate the following:

<u>Required Minimum Qualifications:</u>

- Possession of a Bachelor's Degree in MIS/Computer Science or closely related field, and considerable relevant professional experience in IT area of assignment.
- Minimum of three (3) years' IT experience with at least two (2) years in cyber security, programming or application administration

Required Skills:

- Ability to break down complex problems using a scientific method of troubleshooting issues, resolving and mitigating risk, documenting root cause, and defending analysis.
- Considerable knowledge of the principles, practices, and standards of IAM for systems and applications.
- Ability to communicate effectively, both orally and in writing, with a wide range of technical and business partners regarding complex technology.
- Ability to plan, design, implement, and support the process to provision and deprovision access to MJB systems and applications.
- Ability to provide policy and technical recommendations to management.
- Ability to configure and administer IAM tools and software for the implementation and management of IAM activities for MJB systems and applications.
- Understanding complex problems and being able to solve them using commonly available programming languages (.NET, PowerShell, Python, VBS, etc.)
- Familiarity with security frameworks (NIST, ISO, CIS Controls, etc.)

Desired Skills

- Certifications: CISSP, GSEC, GWAPT, Security+, ITIL
- Application coding experience
- Experience configuring and maintaining Identity Governance tools
- Experience configuring and maintaining Privileged Access Management tools
- Thorough knowledge of tools, hardware, and software in use for IAM.

VIII. Proposal Requirements

- Cover sheet signed by vendor authorized representative and candidate.
- Hourly rate and a total "not to exceed" dollar amount for the proposal.
- Resume of assigned individual demonstrating:
  - Required qualifications.
  - Required and desired skills.
- References: Provide three (3) clients you have assisted with same or similar work efforts
- Conflict of interest statement as it relates to this position.

IX. Statement of Work Evaluation Process

- Skills / Experience (40%)
- Hourly Rate (20%)a
- Interview (40%)

X. Statement of Work Process and Selection Schedule

- Posting Date on MJB Court Public Website - Public Notice: December 9th 2024
- Deadline for Questions: December 10th, 2024
- Posted Response to Questions: December 11th, 2024

- Proposal Submission Deadline: December 12th, 2024
- Proposal Evaluation Begins: Thereafter
- Candidate Interviews: At the convenience of both parties
- Subsequent selection as soon as possible thereafter

a. Amendments

Any amendments to this SOW will be posted on MJB Court Public Website - Public Notice.

b. Questions All questions about this Statement of Work must be submitted in writing via e-mail to the State's sole point of contact identified in this paragraph no later than December 10th, 2024 at 4pm. Other State personnel are not allowed to discuss the Statement of Work with anyone, including responders, before the proposal submission deadline. The State's sole point of contact for questions is:

Erik Reseland
State Court Administrator's Office
25 Rev. Dr. Martin Luther King Jr. Blvd.
St. Paul, Minnesota 55155
Email: Erik.Reseland@courts.state.mn.us
cc: itdprocurementandcontracts@courts.state.mn.us

Timely submitted questions and answers will be posted on the MJB website by December 11th, 2024 at 4pm, and will be accessible to the public and other proposers.

c. Proposal Submission Instructions Proposals must be submitted via e-mail in PDF form no later than December 12th, 2024 4pm to:

Erik Reseland
State Court Administrator's Office
25 Rev. Dr. Martin Luther King Jr. Blvd.
St. Paul, Minnesota 55155
Email: Erik.Reseland@courts.state.mn.us

No facsimile submissions will be accepted.

d. Signatures - The proposal must be signed by in the case of an individual, by that individual, and in the case of an individual employed by a firm, by the individual and an individual authorized to bind the firm.

e. Ink. Prices and notations must be typed or printed in ink. No erasures are permitted. Mistakes may be crossed out and corrections must be initialed in ink by the person(s) signing the proposal.

f. Deadline; Opening; Public Access. Proposals must be received no later than December 12th, 2024 4pm. Proposals, once opened, become accessible to the public. Do not place any information in your proposal that you do not want revealed to the public.

Please also note that if a vendor's proposal leads to a contract, the following information will also be accessible to the public: the existence of any resulting contract, the parties to the contract, and the material terms of the contract, including price, projected term of the contract and scope of work. All documents

accompanying or attached to the proposal, including the proposal, will become the property of the State.

g. Late Proposals. Late proposals will not be accepted or considered.

h. Selection Timeline. Vendor selection will be as soon as possible after the proposal submission deadline.