



**MINNESOTA  
JUDICIAL BRANCH**  
STATE COURT ADMINISTRATOR'S OFFICE

**REQUEST FOR PROPOSALS:**

**Internal and External Assessment of Network, Computer, and Application Environments.**

**I. REQUEST FOR PROPOSALS**

- A. **Defined.** The State of Minnesota –State Court Administrator’s Office (SCAO) is using a competitive selection process (referred to herein as the “Request for Proposals” or “RFP”) to select the vendor responsible for Internal and External Assessment of network, computer and application environments. This is not a bid, but a Request for Proposals that could become the basis for negotiations leading to a contract with a vendor to provide the tool and services described in this document.
- B. **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. The state reserves the right to cancel or withdraw the request for proposals at any time if it is considered to be in its best interest. In the event the request for proposals is cancelled or withdrawn for any reason, the state shall not have any liability to any proposer for any costs or expenses incurred in conjunction with this request for proposals or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. PROJECT OVERVIEW**

- A. **Minnesota Judicial Branch (MJB).** The MJB has 10 judicial districts with 289 district court judgeships, 19 Court of Appeals judges, and seven Supreme Court justices. The MJB is governed by the Judicial Council, which is chaired by Lorie S. Gildea, Chief Justice of the Minnesota Supreme Court. The MJB is mandated by the Minnesota Constitution to resolve disputes promptly and without delay. In 2015, there were more than 1.2 million cases filed in district courts in Minnesota. For more information please visit [www.mncourts.gov](http://www.mncourts.gov).
- B. **State Court Administrator’s Office.** The mission of the State Court Administrator’s Office (SCAO) is to provide leadership and direction for the effective operations of the MJB through support of the Judicial Council, oversight of all SCAO divisions, and coordination of legislative relations, ensuring the provision of sound legal advice, and monitoring branch financial practices through the use of regular internal audits.

The State Court Administrator plans for statewide MJB needs, develops and promotes statewide administrative practices and procedures, oversees the operation of statewide court programs and strategic initiatives, and serves as a liaison with other branches of government.

- C. **Background.** The MJB's commitment to security and industry best practices, state statutes and regulatory considerations, and the need to protect data relating to Minnesota citizens, businesses, and state government, provides the base to issue this RFP seeking to engage an independent, highly qualified, security expert firm to assess potential vulnerabilities from both internal and external forces.

### III. PROJECT GOAL AND SCOPE OF SERVICE

- A. The overall objective of this project is to secure a highly skilled and qualified firm of security experts with at least five (5) years of experience to provide MJB with a network security assessment to scan, investigate, analyze, report and baseline the level of risk associated with any security vulnerabilities, concerns and deficiencies discovered. The process will identify devices on our network that are open to known vulnerabilities without compromising our system. This process must also cause little to no disruption to our users and daily operations.
- B. The responder's approach will utilize industry best practice methodologies and state of the art tools to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential.
- C. The responder will provide a cost breakdown per phase of this project. If the responder proposes additional deliverables it should be clearly documented in the corresponding phase.
- D. The responder will be responsible for various levels of communication to a variety of stakeholder groups and provide complete and comprehensive oral and written reports.
- E. The responder will provide an action plan and recommendations for corrective measures of vulnerabilities and clearly defined mitigation strategies.
- F. The responder will create a roadmap for implementations of defined mitigation strategies for MJB to reduce risks and deficiencies due to security vulnerabilities; as well as compliance to industry standards and best practices to secure MJB systems, applications, information and data.
- G. The responder will recommend and perform regularly scheduled ongoing assessments for up to three (3) years after completion of the original assessment to mark organizational progress regarding implementation of security strategies and progress in vulnerability and risk mitigation.
- H. The responder will make recommendations for policies, procedures and tools to assist MJB in meeting the goal to create more secure systems, applications and overall environment related to IT for staff.
- I. This assessment is to include, but not be limited to:
- i. Conduct an external pentest for MJB's susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets and other

- targeted attack exploits. Evaluate MJB's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- ii. Conduct network architecture and firewall assessment; identify vulnerabilities as a result of configuration issues, segmentation, and firewall design.
  - iii. Review wireless network system components for security vulnerabilities, validating system-specific configurations and known exploits.
  - iv. Validate system-specific configurations and review for known exploits. This includes but is not limited to firewalls, switches and routers, Active Directory, email and file servers, web servers, wireless routers.
  - v. Conduct a web application pentest looking at externally facing applications for vulnerabilities that come about from programming logic and business logic, using manual inspection as well as automated scanning tools.
  - vi. Conduct a review of MJB's tools and appliances designed to mitigate susceptibility to APTs to ensure they are being configured optimally and maximized for threat protection.
  - vii. Conduct internal pivot assessment looking for activities that bad actors or insider threats might perform - attempts to gain access to other systems, identify sensitive information, escalate privileges on the network, and pivot to other areas of the network.
  - viii. Conduct internal network pentest looking for vulnerabilities and testing of computers, devices, databases, systems and networking equipment.
  - ix. Conduct internal phishing assessment of MJB staff to determine the level of threat produced by internal resources and help to create a training plan.

**IV. PROJECT DELIVERABLES** – Each of the following phases will contain deliverables as established in A and B of this section.

A. Project plan:

- Project schedule
- Milestones
- Communications plan
- Issues & decision list
- Regular status reports

B. Scoping sessions to determine breadth and depth of each proposed phases:

- Identify and document tests and activities to be performed
- Identify and document tools to be used to perform activities
- Document findings and results for phase and explanation of determined results
- Recommendations for risk mitigation, industry standard fixes and retesting process;

C. Phase 1: System Reconnaissance:

- Cursory review of MJB systems and applications
- Assess and document high level external view of MJB systems
- Identify and document MJB risk footprint and attack surface;

- D. Phase 2: External Assessment and Pentest:
  - Define items for inclusion
  - Identify testing methodology
  - Document findings and results for phase and explanation of determined results
  - Recommendations for risk mitigation, industry standard fixes and retesting process;
  
- E. Phase 3: Internal Assessment and Pentest:
  - Define items for inclusion
  - Identify testing methodology
  - Document findings and results for phase and explanation of determined results
  - Recommendations for risk mitigation, industry standard fixes and retesting process;
  
- F. Phase 4: Application Assessment and Pentest:
  - Define items for inclusion
  - Identify testing methodology
  - Document findings and results for phase and explanation of determined results
  - Recommendations for risk mitigation, industry standard fixes and retesting process;
  
- G. Phase 5: Staff assessment:
  - Define items for inclusion
  - Identify testing methodology
  - Document findings and results for phase and explanation of determined results
  - Roadmap appropriate security training by MJB employee role. The vendor will create a training plan around security practices and information with recommended education requirements to MJB specific staff classifications. These include business, technology, Justices, Judges, Referees and Magistrates, and contract staff.
  - Recommendations for risk mitigation, industry standard fixes and retesting process;

## V. SUBMISSION REQUIREMENTS.

### A. **General Requirements** – each response must include the following or it may be excluded from moving through to the next phase of response scoring:

1. **Certificate of Insurance.** Each proposal shall contain acceptable evidence of compliance with the workers' compensation coverage requirements of Minnesota Statute § 176.181, subd. 2. Vendor's RFP response must include one of the following: (1) a certificate of insurance, or (2) a written order from the Commissioner of Insurance exempting you from insuring your liability for compensation and permitting him to self-insure the liability, or

(3) an affidavit certifying that you do not have employees and therefore are exempt pursuant to Minnesota Statutes §§ 176.011, subd. 10; 176.031; and 176.041. *See* the sample State contract in Appendix III for details on additional insurance requirements that must be provided upon request of the State.

2. **Affirmative Action Certification.** If the vendor's proposal exceeds \$100,000.00, the RFP response must include a completed Affirmative Action Statement and Certificate of Compliance, which are attached as Appendix I.
3. **Non-Collusion Affirmation.** Vendor must complete the Affidavit of Non-Collusion (Appendix II) and include it with its RFP response.
4. **Contract Terms – acknowledgment of a and b.** The State's proposed contract templates are set forth in Appendix III (contract) and Appendix IV (subcontractor participation agreement). No work can be started until a contract (and where necessary a subcontractor participation agreement), in the form approved by the State Court Administrator's Legal Counsel Division, has been signed by all necessary parties in accordance with state court procurement and contract policies. The templates included in the appendices are sample forms and are not to be interpreted as offers.
  - a. By submitting a response to this RFP, Vendor accepts the standard terms and conditions and contract set out in Appendices III and IV, respectively. Much of the language included in the standard terms and conditions and contract reflects requirements of Minnesota law.
  - b. Vendors requesting additions or exceptions to the standard terms and conditions or contract terms shall submit them with their response to the RFP. A request must be accompanied by an explanation why the exception is being sought and what specific effect it will have on the Vendor's ability to respond to the RFP or perform the contract. The State reserves the right to address nonmaterial requests for exceptions to the standard terms and conditions and contract language with the highest scoring Vendor during contract negotiation.
  - c. The State shall identify any revisions to the standard terms and conditions and contract language in a written addendum issued for this RFP. The addendum will apply to all Vendors submitting a response to this RFP. The State will determine any changes to the standard terms and conditions and/or contract.
5. **Evidence of Financial Stability.** Vendor's RFP must provide evidence of Vendor's financial stability as an indicator of Vendor's ability to provide services irrespective of uneven cash flow. **Financial Stability-Related Trade Secret.** Judicial MJB rules of public access permit vendors to

submit evidence of financial stability as trade secret information according to the following:

- a. The evidence-of-vendor's-financial-stability must qualify as a trade secret under Minn. Statute § 325C.01 or as defined in the common law;
- b. The vendor submits the evidence-of-vendor's-financial-stability on a separate document (but as part of their complete submission) and marks the document(s) containing only the evidence-of-vendor's-financial-stability as "confidential;"
- c. The evidence-of-vendor's-financial-stability is not publicly available, already in the possession of the Judicial MJB, or known to or ascertainable by the Judicial MJB from third parties.

Except for financial stability information submitted in accordance with this section, do not place any information in your proposal that you do not want revealed to the public. Proposals, once opened, become accessible to the public except for financial stability information submitted in accordance with this section. 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 and scope of work.

6. **Evidence of Security Measures.** Vendor's RFP must provide evidence of Vendor's security measures as an indicator of Vendor's ability to provide security for judicial branch records. Security Measures-Related Trade Secret. MJB rules of public access permit vendors to submit evidence of security measures as trade secret information according to the following:
  - a. The evidence-of-vendor's-security-measures must qualify as a trade secret under Minn. Statute § 325C.01 or as defined in the common law;
  - b. The vendor submits the evidence-of-vendor's-security-measures on a separate document (but as part of their complete submission) and marks the document(s) containing only the evidence-of-vendor's-financial-security measures as "confidential;"
  - c. The evidence-of-vendor's-security-measures is not publicly available, already in the possession of the MJB, or known to or ascertainable by the MJB from third parties.

Except for financial stability information submitted in accordance with the prior section and security measures information submitted in accordance

with this section, do not place any information in your proposal that you do not want revealed to the public. The yes/no/N/A responses in the security questionnaire will be considered publicly accessible. Proposals, once opened, become accessible to the public except for financial stability information and security measures information submitted in accordance with the requirements in this document. 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 and scope of work.

**B. Project-Related Submission Requirements: each response must include the following or it may be excluded from moving through to the next phase of response scoring:**

1. A cover sheet including Vendors' contact information, email address, business address, and phone numbers. Your proposal must be signed, 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. This can be done on Vendor informational cover sheet as stated in Project Related Submission Requirements;
2. An overview that reflects the Vendors' understanding of the efforts described in this Request for Proposals and the project deliverables;
3. A detailed explanation of how the Vendor proposes to meet the Project objectives and requirements set forth above, including descriptions of the methodology that will be used and examples of the deliverables that will be produced;
4. The Vendor will provide information regarding each staff person to be assign to the project that includes:
  - i. Name of staff person;
  - ii. Years of experience working in IT Security;
  - iii. Detailed description of security qualifications;
  - iv. All security certifications held by individuals assigned to the project;
5. Any reference to proprietary and confidential tools, middleware, or software that is to be used in the execution of the assessment test can be sealed in an envelope and marked as confidential.
6. Provide a not-to-exceed cost to include identification of the assumptions made and the rationale used to prepare the estimate.

7. A description of completed similar projects that demonstrate the Vendor's experience and area of expertise, including Vendor's ability to provide the stated Deliverables;
8. At least three (3) client references with appropriate contact information that the Vendor has performed the same or similar work for in the past three (3) years and that can attest to vendor ability to complete work as stated;
9. A written statement acknowledging either no conflict of interest or identifying any conflicts of interest as it relates to this project for each of the proposed firm resources that will be assigned to this project;
10. Appendix C – Vendor Security Compliance Questionnaire;

**C. Pricing, Risk of Loss**

1. All prices quoted must be firm and not subject to increase unless otherwise provided for in this RFP. Price reductions must immediately be passed on to the State whenever they become effective. Prices must be quoted in United States currency.
2. Travel, administrative, overhead and other related charges and expenses shall be included in the prices set forth in the proposal.

**VI. PROPOSAL EVALUATION.**

- A. The State will evaluate all complete proposals received by the deadline. Incomplete proposals, late proposals, or proposals sent to any other address will not be considered. In some instances, an interview or demonstration may be part of the evaluation process.
- B. The first part evaluation will be limited strictly to the general submission requirements and project specific requirements as outlined in Section V, A & B.
- C. The second part evaluation of all proposals shall be based upon deriving the "Best Value" for the State. Best Value means achieving an appropriate balance between price and other factors that are key to a particular procurement. A procurement that obtains a low price but does not include other necessary qualities and features of the desired product or service does not meet the Best Value criterion. Factors upon which the proposals will be judged include, but are not limited to, the following:
  1. Vendor's industry and previous experience in performing similar work;
  2. Thoroughness, quality, specificity, robustness, flexibility of Vendor's approach/ methodology;
  3. Cost estimate;
  4. Vendor's product and/or service delivery methodology;

5. Reliability of product or service;
  6. Financial stability of the organization; and
  7. Vendor's past performance and client references.
- D. The State reserves the right to determine, at its sole and absolute discretion, whether any aspect of a proposal satisfactorily meets the criteria established in this RFP.
- E. The State reserves the right to request additional information from Vendors during any phase of the proposal evaluation process. During the evaluation and selection process, the State may require the presence of Vendor's representatives at a vendor conference. During a vendor conference, a vendor may be asked to provide a demonstration of the product and/or to answer specific questions. Vendors are required to travel at their own expense to for the demonstration of the product and answer questions. Notification of any such requirements will be given as necessary.
- F. The State may elect not to award a contract solely on the basis of this RFP, and will not pay for the information solicited or obtained. The information obtained will be used in determining the alternative that best meets the needs of the State.

## **VII. SUBMISSION OF PROPOSALS.**

- A. **Proposal Timeline.**
1. Posting Date on State MJB Website [MJB Court Public Website - Public Notice](#) : Wednesday, March 30, 2016.
  2. Questions Due: Monday, April 4, 2016, by 3:30 P.M.
  3. Answers Posted: Monday, April 11, 2016, by 3:30 P.M.
  4. Proposal Submission Deadline: Monday, April 18, 2016 by 3:30 P.M
  5. Vendor conferences will be scheduled if needed.
  6. Subsequent selection as soon thereafter as possible.
- B. **Amendments.** Any amendments to this RFP will be posted on the MJB website.
- C. **Questions.** All questions about this RFP must be submitted in writing via email to the State's sole point of contact identified in this paragraph no later than Monday, April 4, 2016, by 3:30 P.M. Other court personnel are not allowed to discuss the Request for Proposals with anyone, including responders, before the proposal submission deadline.

Jodie Monette, Security Architect  
[jodie.monette@courts.state.mn.us](mailto:jodie.monette@courts.state.mn.us)

D. **Answers to Questions.** Timely submitted questions and answers will be posted on the Judicial MJB website by the end of the day on Monday, April 11, 2016, by 3:30 P.M., and will be accessible to the public and other proposers.

E. **Sealed Proposal and Submittal Address.** Your proposal must be submitted in writing Monday, April 18, 2016, by 3:30 P.M., in a sealed envelope to:

Jodie Monette, Security Architect  
State Court Administrator's Office  
25 Rev. Dr. Martin Luther King Jr. Blvd.  
St. Paul, Minnesota 55155  
jodie.monette@courts.state.mn.us

The submission must include both four (4) paper copy and one (1) electronic PDF copy either on disc or flash drive. No facsimile submissions will be accepted. Proposals delivered in person to State Court Administration should be presented to the First Floor receptionist and date/time stamped by the receptionist.

F. **Signatures.** Your proposal must be signed, 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. This can be done on vendor informational cover sheet as stated in Project Related Submission Requirements.

G. **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 signing the proposal.

H. **Deadline; Opening; Public Access.** Proposals must be received no later than Monday, April 18, 2016, 3:30 P.M. Proposals will be opened the following business day and once opened become accessible to the public (except financial stability information submitted as a trade secret in accordance with the instructions in Section V(A)(6) & confidential proprietary tools, middleware and software in Section V(B)(5) of this RFP). With the exception of evidence-of-vendor's-financial-stability trade secret information submitted in accordance with the instructions in Section V(A)(6) & confidential proprietary tools, middleware and software in Section V(B)(5) of this RFP, do not place any information in your proposal that you do not want revealed to the public. All documentation shipped with the proposal, including the proposal, will become the property of the State.

I. **Late Proposals.** Late proposals will not be accepted or considered.

J. **Selection Timeline.** Selection will be as soon as possible after the proposal submission deadline.