Attachment A

to

RFP No. 4350

Mississippi Department of
Information Technology Services

Security Risk Assessment Services

ITS Project No. 43562

TABLE OF CONTENTS

Attachment A to RFP No. 4350
ITS – Security Risk Assessment Services

I. GENERAL

A. How to Respond

1. Beginning with Item 20, label and respond to each outline point in this section as it is labeled in the RFP.
2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items to which they disagree.
3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.
4. "WILL COMPLY" indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or Vendor's proposed solution must comply with a specific item or must perform a certain task.
5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V of RFP No. 4350, for additional instructions regarding Vendor exceptions.)
6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.
8. In Attachments AI, AII, AIII, and AIV of this RFP, Vendors must label and respond to each outline point with "A", "E", or "X" dependent on the Vendor response. "A" should be used when the Vendor agrees or will comply with the requirement. "E" should be used if the Vendor is unable to meet the requirement but is able to provide an alternative solution. This alternative solution must be defined in Section V, Proposal Exception Summary. If a Vendor cannot respond with "A" or "E", then the Vendor must respond with "X" to indicate that the service is not available, or Vendor is not capable of providing.

B. Mandatory Provision in Technical Requirements for this RFP

9. Certain items in the technical specifications of this RFP are MANDATORY. Vendors are specifically disallowed from taking exception to these mandatory requirements, and proposals that do not meet all mandatory requirements are subject to immediate disqualification.
10. Mandatory requirements are those features classified as "M" (Mandatory) in the Attachment A and Attachment B MDHS System RTM documents. Meeting a mandatory requirement means the Vendor has provided a detailed response that demonstrates that the Vendor meets the qualifications and experience required and/or the requested functionality exists in the base solution at time of proposal submission.

C. Overview and Background

11. In the 2017 Legislative Session, the Mississippi Legislature passed House Bill 999 that created a new section of Mississippi Code (25-53-201) for the advancement of the state government enterprise approach to cybersecurity. To fulfill the statutory requirements in Mississippi Code Ann. 25-53-201 for cybersecurity, the State of Mississippi shall have

a comprehensive cybersecurity program (the Enterprise Security Program) to provide coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services, and development of policies, standards, and guidelines. ITS is responsible for administering the Enterprise Security Program to execute the duties and responsibilities of Mississippi Code Ann. 25-53-201.

12. The security and risk assessment services resulting from this RFP will be available to state agencies as additional services to the Enterprise Security Program, acting by and through ITS. "Agency" is defined as "all the various State agencies, officers, departments, boards, commissions, offices and institutions of the State" and includes the State's Institutions of Higher Learning (IHLs).

13. ITS' legislative charge is to leverage enterprise security solutions to provide services to state agencies when it is determined that such operation will improve the cybersecurity posture in the function of any agency, institution, or function of state government. In doing so, ITS will leverage the total aggregate buying power of State government to obtain both best pricing and highest quality of service from Vendors on behalf of State government.

14. The contracts awarded under this RFP will be available for use by different categories of public entities in the State of Mississippi. Agencies/entities wishing to use this award will follow the Instructions for Use document that will be published on the ITS website after this procurement is awarded.

15. The Mississippi Department of Information Technology Services (ITS) is seeking the services of qualified Vendors to provide comprehensive security and risk assessment services for the information technology (IT) assets used by ITS and public government entities of Mississippi. The comprehensive security and risk assessment services are needed to investigate, identify, measure, and prioritize the potential risks that exist on the IT assets for the State of Mississippi. These services must incorporate the use of human interaction as well as automated tools to assess and report these vulnerabilities. In addition to providing information on the potential risks, recommendations must be provided that will allow agencies to understand their exposure and take precise measures to mitigate it.

16. The comprehensive set of security and risk assessment services are comprised of four types of assessment service offerings: 1) Cloud Compliance Services; 2) Penetration Testing Services; 3) Security Risk Assessment Services; and 4) Security Program Assessment Services. Vendors have the option of submitting proposal responses to one or multiple types of assessment service offerings.

    - Cloud Compliance Services should include services to review cloud and offsite hosting providers for validation that the providers are adhering to the security requirements of the agency as well as the State's Enterprise Security Policy and Enterprise Cloud and Offsite Hosting Security Policy.

    - Penetration Testing Services should include techniques to prove vulnerabilities exist and demonstrate the security exposures that occur when they are exploited.

    - Security Risk Assessment Services should include techniques that examine defined system assets, applications, networks, policies, security configurations, and operational processes and procedures to discover real or potential vulnerabilities and threats. Security Risk Assessment Services should also

include techniques that identify active assets and their associated ports and services, and analyzing them for potential vulnerabilities.

- Security Program Assessment Services should include risk and compliance services for assessing the maturity of a security program against a set of criteria. Services should also include assistance in developing a standard set of criteria of which security programs will be assessed.

17. This RFP is broken down into four distinct categories for response and evaluation. The four categories are (I) Cloud Compliance Services, (II) Penetration Testing Services, (III) Security Risk Assessment, and (IV) Security Program Assessment. Vendors must provide a response to Section VII Technical Specifications with the categories in which they wish to provide a response. Vendors DO NOT have to provide a response to all 4 categories.

18. ITS anticipates receiving proposals and awarding to multiple qualified Vendors to develop a pool of vendors for the following categories: (I) Cloud Compliance, (II) Penetration Testing Services, and (III) Security Risk Assessment Services. Each awarded category will have its own vendor pool for use by State agencies. Each agency will solicit quotes from the awarded vendors in each respective category and award the vendor with the lowest cost. The awarded Vendor and Agency will execute a Statement of Work that details what services will be provided.

19. Category IV: Security Program Assessment will be awarded to one vendor.

II. FUNCTIONAL AND TECHNICAL REQUIREMENTS

D. Functional and Technical Requirements

20. In order to accurately and completely document functional requirements, ITS has identified four (4) functional categories wherein Vendors may respond. For the functional and technical requirements relevant to this procurement, refer to Attachments AI, AII, AIII, and AIV, which are incorporated herein by reference and are considered integral to this RFP. ATTACHMENTS AI, AII, AIII, and AIV are posted on the same website location as this RFP No. 4350, and the link is located directly beneath the link for RFP No. 4350.

21. Vendor must complete and return the Attachment A spreadsheet for the categories in which they wish to respond. It should be understood that Vendors are not required to respond to every category listed below. Vendors should respond only to the categories desired. Vendor must respond by typing “YES” beside each category or categories they are proposing.

    a. Attachment AI, Category I - Cloud Compliance
    b. Attachment AII, Category II – Penetration Testing
    c. Attachment AIII, Category III - Security Risk Assessment
    d. Attachment AIV, Category IV – Security Program Assessment

22. Attachments AI – AIII: Vendor must complete the first tab in each spreadsheet, which contains the Technical Specifications – Requirements Matrix for each Category as indicated, and Cost Submission tabs.

23. Attachment AIV – Vendor must complete the first tab in the spreadsheet, which contains the Technical Specifications – Requirements Matrix for Category IV, as well as the Cost Submission and Appendix A tabs.

E. Vendor Qualification and Experience

24. Organization Description – The Vendor must provide a description of the organization to include the following information:
    a. Corporate information to include Parent Corporation and any subsidiaries;
    b. The name of the state of incorporation;
    c. Location of Vendor's principal office and the number of executive and professional personnel employed at this office;
    d. Location of the office that will be servicing this project;
    e. Disclosure of any company restructurings, mergers, and acquisitions in the past three years that have impacted any products the Vendor sold, serviced, and supported;
    f. A copy of the corporation's most recent annual report showing the Vendor's financial stability. The Vendor's annual report can be submitted electronically with the proposal response; and
    g. Number of years the company has been in business.

25. Experience
    a. The Vendor must discuss experience of company in furnishing the proposed services requested in response to the RFP.
    b. The Vendor must provide detail demonstrating the ability to provide the proposed services requested in response to the RFP.
    c. The Vendor must have experience and understanding of state and local government contracting and be responsive to its unique requirements.
    d. The Vendor must identify how many paid customers utilized the services being proposed:
        1. Cloud Compliance Services
            a. Public Sector
            b. Private Sector
        2. Security Risk Assessment Services
            a. Public Sector
            b. Private Sector
        3. Penetration Testing Services
            a. Public Sector
            b. Private Sector

26. Staff Qualifications
    a. The Vendor must identify the executive and professional personnel who will be assigned to the security/risk assessment projects and state their duties and responsibilities.

b. The Vendor must provide resumes and references for the Vendor's proposed single Point of Contact (SPOC) and lead/primary IT security resources assigned to the project. Resumes must reflect qualifications and recent experience relevant to the scope of the work indicated in this RFP and the area of the project that the proposed individual will be assigned.

c. The Vendor must state at the top of each resume for each individual assigned to the project.

   1. The number of years of directly related experience to the services they will be providing; and

   2. Relevant certifications and/or security clearance/classifications. Vendor must provide references and proof of certification.

d. The State reserves the right to approve all individuals assigned to this project.

e. The Vendor must agree to allow the proposed staff, including any subcontractors, to be subject to background checks. The Vendor must describe the background verification process used in the hiring of its management staff and its individual consultants.

F. Billing

27. Categories I - III

    a. The Vendor must be able to direct bill all State agencies and Governing authorities (e.g. community/junior colleges, county boards of supervisors, school districts, and municipalities) for services rendered in Categories I – III.

28. Category IV

    b. The Vendor must be able to bill Governing authorities directly for services rendered in Category IV.

G. Master Security Consulting Services Agreement

29. This Section details contract requirements that apply to all awarded Vendors.

30. The words "agreement" and "contract" shall be used synonymously.

31. The Master Security Consulting Services Agreement contains the minimum terms and conditions which are necessary to do business with the State.

32. **MANDATORY** - Due to the need for uniformity among the Vendors, all awarded Vendors for Categories I, II, and III must be willing to execute the Master Security Consulting Services Agreement with no exceptions.

33. Vendors responding to Category IV may take exceptions to the Master Security Consulting Services Agreement as described in Section V, Proposal Exceptions.

34. The inclusion of this Agreement does not preclude ITS from, at its sole discretion, including and/or negotiating additional terms and conditions with selected Vendors.

35. All contracts are subject to availability of funds of the acquiring state entity.

36. A separate contract for each awarded Category will be executed with each awarded Vendor.

37. For Categories I, II, and III, Vendor will only return two (2) copies of the executed signature page (for each service proposed). Both copies must be executed with original signatures by the authorized officer of your company.
    a. Do not return the entire agreement.
38. Once a Vendor has been approved for the pool, ITS will merge the signature pages with the full agreement and execute both copies. One (1) executed original will be returned to the Vendor.

III. PERFORMANCE MANAGEMENT

H. Cloud or Offsite Hosting Requirements

39. Data Ownership - The State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State 's written request.
40. Data Protection - Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:
41. All information obtained by the Vendor under this contract shall become and remain property of the State.
42. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.
43. Data Location - The Vendor shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Vendor will permit its personnel and contractors to access State data remotely only as required to provide technical support.

    a. Encryption

        i. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

        ii. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

1. The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).

2. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.

3. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.

4. At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.

5. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.

6. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.

7. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.

9. In the event the Vendor fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

b. Breach Notification and Recovery -

Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

44. Notification of Legal Requests - The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related

to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

45. Termination and Suspension of Service - In the event of termination of the contract, the Vendor shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of State data.

46. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any State data.

47. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90 day period, the Vendor shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in Item 94. Within this 90 day timeframe, Vendor will continue to secure and back up State data covered under the contract.

48. Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

49. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.

50. Background Checks - The Vendor warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.

51. Security Logs and Reports - The Vendor shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

52. Contract Audit - The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.

53. Sub-contractor Disclosure - The Vendor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or

similar agreement with the Vendor, who will be involved in any application development and/or operations.

54. Sub-contractor Compliance - The Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

55. Processes and Procedures - The Vendor shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing — the State and the Vendor shall understand each other's roles and responsibilities.

56. Operational Metrics - The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:

    a. Advance notice and change control for major upgrades and system changes
    b. System availability/uptime guarantee/agreed-upon maintenance downtime
    c. Recovery Time Objective/Recovery Point Objective
    d. Security Vulnerability Scanning

I. Other Requirements

57. If any component(s) necessary for operation of the requested system is omitted from Vendor's proposal, Vendor must be willing to provide the component(s) at no additional cost.

58. ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed solution/services. Vendors must specify, here, what additional components/services may be needed and are proposed in order to provide comprehensive security risk assessment services.