

**EXHIBIT A-1**  
**Statement of Work Template**

**STATEMENT OF WORK FOR A MILESTONE, DELIVERABLE OR SERVICE-BASED PROJECT**  
**BETWEEN**  
**STATE OF MISSISSIPPI, Department of Mississippi Public Employees' Retirement System**  
**AND**  
**GUIDESOFT, INC., d/b/a KNOWLEDGE SERVICES**  
**AND**  
**Ciber Global LLC.**

Authorization for work performed pursuant to this Statement of Work "SOW" is granted under the terms of the Master Consulting Services Agreement between GuideSoft, Inc. d/b/a Knowledge Services and Mississippi Department of Information Technology Services.

**INTRODUCTION**

PERS of Mississippi is seeking to obtain the services of a cybersecurity consulting firm, to provide consultation and guidance with regard to implementation of the CIS security standards, our incident response planning, and the continued development and management of our data and systems security strategy. The firm's consultant(s) will report to both the PERS CIO and the SDA of Administrative Services and offer counsel and guidance to them. Additionally, the consultant(s) will provide advice to members of the PERS' cybersecurity team which has been meeting bi-monthly to discuss security related activities and review the status updates of our security initiatives. (As of June 30, 2019, PERS reported over 300,000 members and approximately \$28.6 billion in investments.)

**SCOPE OF WORK**

PERS has identified the following cybersecurity consulting activities to be performed utilizing the established Knowledge Services Contract:

1. Reporting to the SDA and CIO, provide technical advice, updates and progress reports with regard to PERS systems security work including CIS standards, industry best practices, and advice on how to prioritize and implement certain steps. Additionally, the consultant will offer feedback and guidance to members of the cybersecurity team as they continue to move forward with security initiatives in accordance with security industry standards.
2. Review, advise, and confer with the PERS SDA and CIO with regard to the agency's system security initiatives.
3. Provide a quarterly report to the SDA and CIO which includes a high-level assessment of PERS' current progress in building and maintaining a mature cybersecurity program that provides adequate protection from contemporary cybersecurity threats, as well as identifying emerging cyber risks and threats for which a response is needed.
4. Assist the PERS' cybersecurity team in establishing goals (with target dates) of all CIS controls and provide coaching on how to effectively prioritize and manage implementation activities.
5. Participate in scheduled cybersecurity team meetings and provide feedback, advice, and guidance concerning security related issues and topics. Consultant may participate on-site, by phone, or by Microsoft Teams or similar products such as Zoom.
6. Provide review, consultation and advice related to security policies, procedures and documentation developed and maintained by PERS, including the incident response plan. Provide sample policies and content for consideration.
7. Provide subject matter experts to ensure best practice cyber security readiness and compliance in all areas such as firewall management, administrative privileges management, data and event logging and analysis, and hardening standards, etc.
8. Upon request by PERS' cybersecurity team members, provide consultation and assistance, including working through detailed documentation associated with certain CIS Controls, to help determine a practical approach for implementation and achieving an acceptable level of compliance based upon industry standards.

## **PERIOD OF PERFORMANCE**

Start date: August 17, 2020 with expected duration of three (3) years with possible extension. PERS reserves the right to terminate this agreement with a 30-day notice should funding be lost/decreased and/or the project is discontinued for any reason.

## **PLACE OF PERFORMANCE**

Work performed will be a combination of off-site and on-site activities based upon PERS approval of scheduled work.

<b>Project Name:</b>	Cyber Security Consulting Services	<b>Posting ID#:</b>	70911
<b>Project Start Date:</b>	August 17, 2020	<b>Project End Date:</b>	August 17, 2023
<b>Contractor Name</b>	<b>Contractor Title</b>	<b>All-encompassing hourly rate</b>	
Ali Baig	Security Lead / Specialist	\$130.00	
Don Beyer	Security Lead / Specialist	\$130.00	
Rebecca Kettler	Senior Security Consultant	\$130.00	

*A change order will be required for any modifications to the project (Including project scope/project cost). The change order must be created by Knowledge Services, based on the approved change order justification received by VENDOR (approved by AGENCY). The change order must be signed by AGENCY, VENDOR, and Knowledge Services prior to the vendor receiving clearance to move forward with the requested changes.*

## **ACCEPTANCE CRITERIA**

Based upon monthly intervals of work completed, the Vendor shall notify Knowledge Services Program Manager and indicated an invoice is ready for submittal into VMS dotStaff. Once the milestone has been created in dotStaff Vendor will submit invoices into VMS dotStaff indicating the number of hours worked by each team member or resource and reference the services to which the hours of work pertain. The invoice must reflect the contractual blended rate for all services rendered. Any required reports will also be submitted into dotStaff at this time. Upon PERS review and acceptance of the work specified in the invoice, PERS will approve the invoice by accepting the bid in dotStaff. In the event PERS is dissatisfied or disagrees with the invoice submitted, PERS will reject the invoice in dotStaff and provide the Vendor with their findings. The Vendor shall make necessary corrections and submit the corrected invoice and/or report for approval and payment. PERS reserves the right to terminate the SOW contract with the selected vendor with a thirty-day notice of termination. PERS will submit payment for all approved invoices for work completed prior to the date of termination specified in the notice of termination of the agreement.



## OTHER REQUIREMENTS

Consultant team must possess the following required skills/experience:

1. Eight years or more experience providing cybersecurity consulting to complex organizations.
  2. Eight years or more experience in Systems and Network Administration; and
  3. Eight Years or more experience providing implementation of security frameworks such as CIS, NIST, and ISO.
  4. Extensive cybersecurity experience with securing enterprise resource planning (ERP) systems from companies such as Oracle, Microsoft, and SAP.
  5. Preference will be given to candidates whose staff members possess one or more of the following certifications:
    - a. IAPSC - Certified Security Consultants (CSC)
    - b. (ISC)<sup>2</sup> - Certified Information Systems Security Professional (CISSP)
    - c. ISACA – Certified Information Security Manager (CISM)
  6. Consideration will be given as to the size and complexity of current and former clients.
- If your staff members possess other Industry Standard Security Certifications or they do not possess any certifications, please specify this information when submitting your bid.

For the faithful performance of the terms of this Statement of Work, the parties hereto have caused this Statement of Work to be executed by their undersigned authorized representatives.

Customer Agency Name

PERS of MS

Authorized Signature

H. RAY HIGGINS, Jr.

Printed Name

Executive Director

Title

8/5/2020

Date

Guidesoft Inc., d/b/a Knowledge Services

Katie Belange

Katie Belange (Aug 11, 2020 14:20 CDT)

Authorized Signature

Katie Belange

Printed Name

Corporate Counsel

Title

Aug 11, 2020

Date

Vendor Name

Authorized Signature

SUTBIR KANDHAWA

Printed Name

Vice President

Title

8-10-2020

Date

Guidesoft Inc., d/b/a Knowledge Services - Legal

Doreen DeLancy

Authorized Signature

Doreen DeLancy

Printed Name

Program Manager

Title

August 4, 2020

Date