REQUEST FOR PROPOSAL
Managed Security Services

Issued December 21, 2018

Responses due via email
by 4:30pm CT on January 25, 2019
Table of Contents

I. Introduction ............................................................................................................................................................... 3
II. Description of SURS ................................................................................................................................................. 3
III. Services Required .................................................................................................................................................... 4
IV. Minimum Qualifications ........................................................................................................................................ 5
V. Proposal Content ...................................................................................................................................................... 5
   Cover Letter .......................................................................................................................................................... 5
   Statement of Minimum Qualifications ................................................................................................................. 5
   Reference Checks .................................................................................................................................................. 5
   Questionnaire ....................................................................................................................................................... 5
   Supplemental/Technical Questionnaire ............................................................................................................... 5
   Fee Proposal ......................................................................................................................................................... 5
   Contract ................................................................................................................................................................ 6
   Project Schedule ................................................................................................................................................... 6
VI. Submission of Proposals ....................................................................................................................................... 6
VII. Evaluation Process .................................................................................................................................................. 6
   Pre-Evaluation Review .......................................................................................................................................... 6
   Proposal Evaluation .............................................................................................................................................. 6
VIII. Anticipated Timeline and Contact Information ............................................................................................ 8
IX. Submission Process ................................................................................................................................................. 8
   Deadline ................................................................................................................................................................ 8
   Withdrawal ........................................................................................................................................................... 8
   Questions .............................................................................................................................................................. 8
X. General Conditions .................................................................................................................................................. 9
   Freedom of Information Act Disclosure ........................................................................................................... 9
   Redacted Version of RFP Response ................................................................................................................... 9
   Ordinary Course of Business Communications Allowed ............................................................................. 9
   SURS Quiet Period Policy ................................................................................................................................... 10
   Rights Reserved .................................................................................................................................................. 10
   Equal Opportunity .............................................................................................................................................. 11
   Terms and Conditions ........................................................................................................................................ 11
Appendix A: Statement of Minimum Qualifications ............................................................................................... 11
I. Introduction

The State Universities Retirement System (“SURS” or the “System”) is seeking proposals from qualified vendors to provide Managed Security Services to supplement our existing in-house security hardware and software.

All forms/required documents needed for submitting a Request for Proposal (“RFP”) are available on the SURS website at www.surs.org.

A proposer’s preparation and submittal of a proposal or subsequent participation in presentations or contract negotiations creates no obligation on the System to award a contract or to pay any associated costs. All proposals and related materials will be retained by the System and will be subject to disclosure as required in accordance with the Illinois Freedom of Information Act.

II. Description of SURS

SURS is the administrator of a cost-sharing, multiple employer, public employee retirement system that provides retirement, survivor, disability and death benefits to employees of Illinois state universities, community colleges, and certain other affiliated organizations and agencies. SURS was created in 1941, by an act of the Illinois General Assembly, and is governed by the Illinois Pension Code (40 ILCS 5/15-101 et seq.). SURS provides benefit services to over 230,000 members who work for 61 employers. SURS is responsible for investing assets of more than $19 billion in a diversified portfolio of U.S. and foreign stocks, bonds, real estate and alternative investments. SURS also administers a defined contribution plan, the Self-Managed Plan, which currently has assets of approximately $2.2 billion. Northern Trust serves as SURS’ Master Trustee Custodian.

An elected and appointed, eleven-person, Board of Trustees, governs SURS. The chairperson of the Board of Trustees is, by statute, the chairperson of the Illinois Board of Higher Education. Five members of the Board are
appointed by the governor of the state of Illinois. The remaining six members of the Board are elected by participating members (four individuals) and annuitants (two individuals). Our trustees serve six-year terms. SURS is funded by participant payroll deductions and annual employer contributions provided by the state of Illinois. By statute, SURS is defined as a “body politic and corporate” created by Article 15 of the Illinois Pension Code.

SURS currently employs approximately 132 staff, located in 2 offices in Champaign and Naperville, Illinois. Two SURS employees are in the Naperville office. The remaining SURS employees are situated in the Champaign office.

A copy of SURS’ most recent Comprehensive Annual Financial Report (CAFR) is available for review, or to download, at www.surs.org.

The Illinois Governmental Ethics Act, 40 ILCS 420, provides guidelines for ethical practices concerning state and local pension plans. Respondent providers should be familiar with the provisions of this Act.

Section 1-109.1(6) of the Illinois Pension Code (40 ILCS 5/1-109.1(6)) encourages Illinois public pension systems like SURS to utilize businesses owned by “minorities”, “women”, and “persons with disabilities” for all contracts and services, as those terms are defined in the Business Enterprise for Minorities, Women, and Persons with Disabilities Act (“BEMWPD”, 30 ILCS 575). Additionally, Section 1-109.1(10) of the Illinois Pension Code (40 ILCS 5/1-109.1(10)) sets an aspirational goal of not less than 20% of contracts awarded to such businesses for “information technology services”, “accounting services”, “insurance brokers”, “architectural and engineering services”, and “legal services” as defined by the BEMWPD. Accordingly, businesses that meet these definitions are strongly encouraged to submit responses to this RFP.

A section of the Illinois Procurement Code concerning prohibitions of political contributions for vendors, 30 ILCS 500/50-37, may or may not apply to SURS service providers. However, each service provider should be familiar with the provisions of this section and comply with this section if the service provider deems it appropriate.

Further legal requirements that vendors should be familiar with are contained in the Addendum to Contract under Appendix D.

III. Services Required

The State Universities Retirement System (SURS) is requesting proposals for Managed Services Solutions to acquire, implement and co-monitor a solution that provides Threat Monitoring & Cyber-Attack Defense, SIEM & Log Management, Incident Response & Event Investigation, Threat Protection and Vulnerability Management. Co-management of our firewall is a requirement. The ability to provide incident response and forensic services is also a consideration. A multi-year contract will be required. Refer to Appendix E for a more detailed account of requirements.

Current Environment: SURS is nearing the renewal period with our contracted Managed Security Service Provider (MSSP). The current MSSP provides services and management of Security Information and Event Monitoring (SIEM) services with trained security expertise on a 24/7 basis. A variety of systems are monitored, approximately 20 of which are Cisco switches and routers, Microsoft Servers, and a pair of high availability Palo Alto firewalls. Additionally, there are 4 IBM iSeries systems being monitored. During normal working hours, the number of events per second is about 150. In addition, we are expanding our environment to Office 365 and any services that are related would be considered a value-add.
IV. Minimum Qualifications

- The responder’s key professionals and/or organization must not have material conflicts with the SURS Board.
- A minimum of 5 years in business providing Managed Security Services.
- Must maintain a staff of certified security professionals that are available 24/7/365.

V. Proposal Content

At a minimum, the proposal must include the following information to be considered for the engagement. For ease of review, each requirement should be addressed separately.

Cover Letter
A cover letter, which will be considered an integral part of the proposal package, in the form of a standard business letter, must be signed by an individual authorized to bind the proposer contractually. This cover letter must indicate the signer is so authorized and must indicate the signer’s title or position. An unsigned proposal will be rejected. The cover letter must also include:

a. A statement that the proposal meets all requirements of this RFP, and that the offer tendered by the proposal will remain in full force and effect until and may be accepted by SURS at any time prior to 30 days beyond the deadline for submittal.

b. A disclosure of any current business relationship or any current negotiations for prospective business with SURS, or with any member of the Board of Trustees or SURS staff, or any party currently rendering services to SURS.

c. A statement that the proposer acknowledges that all documents submitted in response to this RFP may be subject to disclosure under the Illinois Freedom of Information Act and/or the Illinois Open Meetings Act.

Statement of Minimum Qualifications
Proposers must complete and return the Minimum Qualifications Certification in the form contained in Appendix A.

Reference Checks
Reference checks will be conducted for each finalist. Please include at least 3 references, public sector experience preferred.

Questionnaire
The questionnaire contained in Appendix B to this RFP must be completed and returned as part of the proposal.

Supplemental/Technical Questionnaire
Please complete the Supplemental Questionnaire included with this RFP and return with your RFP response.

Fee Proposal
Proposers must submit a proposal in the format prescribed in Appendix C. Any deviation from the prescribed format which in the opinion of SURS is material and may result in the rejection of the proposal. The proposed
fee shall include all costs and expenses for providing the services and equipment as described in this RFP, and any agreed-upon extended warranties that are associated with initial installation. Once finalists are selected, fees may be subject to a “best and final” offer process to be determined at the discretion of the System.

The fee proposal must expressly state that the proposed fees are guaranteed for the term of any resulting contract.

**Contract**
This Request for Proposal is neither a contract nor meant to serve as a contract. It is anticipated that one or more of the proposals submitted in response to this Request for Proposal may be selected as the basis for negotiation of a contract with the proposer. Such a contract is presently contemplated to contain, at a minimum, the terms of the proposal submitted, as finally negotiated and approved by the System. SURS reserves the right to negotiate additions, deletions, or modifications to the terms of proposals submitted. However, the terms contained in Appendix D, Addendum to Contract, must be agreed to and accepted by the candidate or organization selected to perform the work contemplated by this RFP.

**Project Schedule**
The submission must include a preliminary project schedule based on the number of calendar days required to perform the work following the award of the contract. The work contemplated by this RFP must be completed on or before March 31, 2019 and only responders who can meet that deadline will be considered for this project.

**VI. Submission of Proposals**

All proposals must be received no later than the deadline stated in the Anticipated Timeline and Contact Information section. Submissions must be made via email to the identified contact person by the stated deadline. **Only email submissions will be accepted.**

The proposals become the property of SURS upon submission. All costs for developing proposals and attending presentations and/or interviews are entirely the responsibility of the proposer and shall not be chargeable to SURS.

Only one proposal from an individual, firm, partnership, corporation, or combination thereof, will be considered for this assignment.

**VII. Evaluation Process**

**Pre-Evaluation Review**
All proposals will be reviewed to determine if they contain all the required submittals specified in this RFP. Those not submitting all required information in the prescribed format will be rejected.

**Proposal Evaluation**
All proposals received by the SURS representative on or before the deadline listed above will be reviewed to determine whether they meet the minimum requirements of this RFP.

All proposals received by deadline and pass the pre-evaluation review will undergo an evaluation process conducted by SURS staff. They will be reviewed to determine whether they meet the requirements of this RFP. SURS will consider the following factors in the evaluation process, ranked in no specific order, and will render a decision based on the perceived best fit and best value for the engagement. Fees will be one of the
determining factors in this decision but will not be the primary determinative. Proposals will be evaluated based on criteria including:

- Understanding of the services requested
- Timeline for recommended solution to be implemented
- Proposed methodology and work plan to be used in the process
- Proposed deliverables (products/services)
- Relevant knowledge, experience and qualification of firm and team members including established record of success in similar work
- Commitment to diversity
- Overall Viability (Business Unit, Financial, Strategy, Organization)
- Willingness to negotiate contract terms
- Independence
- Sales Execution
- Warranty
- Cost and overall value proposition
- Ability to scale as needs change
- References, Market Responsiveness, Record
- Customer Experience
- Operations Infrastructure
- Responses to the Supplemental Technical Questionnaire
- Adherence to RFP submission requirements

Proposals that contain false or misleading statements or that provide references which do not support an attribute or condition claimed by the proposer will be rejected. Issuance of the Request for Proposal creates no obligation to award a contract or to pay any costs incurred in the preparation of a proposal. Nothing in this RFP or any resulting contract shall preclude SURS from procuring services similar to those described herein from other sources.

During the evaluation process, proposers may be requested to provide additional information and/or clarify contents of their proposal. Other than information requested by SURS, no proposer will be allowed to alter the proposal or add new information after the filing date.

As part of the final determination SURS may want to visit a respondent’s Security Operations Center.

Once finalists are selected, fees may be subject to a “best and final” offer process to be determined at the discretion of the System.
### VIII. Anticipated Timeline and Contact Information

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet Period Begins</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>RFP Issued</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Deadline for Responder Questions</td>
<td>January 11, 2019</td>
</tr>
<tr>
<td>Response to Questions</td>
<td>January 15, 2019</td>
</tr>
<tr>
<td><strong>RFP Responses due 4:30 p.m. CT</strong></td>
<td>January 25, 2019</td>
</tr>
<tr>
<td>Evaluations and Candidate Interviews</td>
<td>January 28 – February 15, 2019</td>
</tr>
<tr>
<td>Anticipated Project Start Date</td>
<td>March 1, 2019</td>
</tr>
</tbody>
</table>

SURS may extend these deadlines at its discretion. Any such extensions will be posted to the SURS website.

**SURS RFP Contact Information**
- Procurement Officer
  - Procurement_Officer@surs.org
- SURS
  - 1901 Fox Drive
  - Champaign, IL 61825-2710

### IX. Submission Process

#### Deadline
To be considered for selection, proposals **must be received via e-mail in Adobe Acrobat format** at Procurement_Officer@surs.org no later than 4:30 p.m. CT, January 25, 2019. Please reference the “Managed Security Services RFP Response - Name of Responder” in your communications. An email confirmation will be sent confirming receipt of the proposal.

#### Withdrawal
A proposal may be withdrawn any time prior to the deadline by written notification signed by the individual applicant or authorized agent of the firm and received at Procurement_Officer@surs.org no later than the deadline of 4:30 p.m. CT, January 25, 2019. Please reference the “Managed Security Services RFP Response - Name of Responder” in your communications. An email confirmation will be sent confirming withdrawal of the proposal. The proposal may be resubmitted with any modifications no later than the deadline. Modifications offered in any other manner will not be considered.

#### Questions
To clarify any issues in this Request for Proposal, SURS will respond only to questions that are presented in writing via e-mail to Procurement_Officer@surs.org. All questions should be submitted to SURS by 4:30 p.m. CT, January 11, 2019. Please reference the “Managed Security Services RFP Response - Name of Responder” in your communications. These questions will be consolidated into a single Q&A document and responded to by
SURS on, or about, January 15, 2019. The Q&A document will be posted on the SURS web site at www.surs.org/rfp without indicating the source of the query.

X. General Conditions

Freedom of Information Act Disclosure

All materials submitted in response to the RFP become property of SURS. Proposals remain confidential during the selection process. However, upon completion of the selection process, all responses, including that of the individual, vendor or firm selected, will be a matter of public information and will be open to public inspection in accordance with the state of Illinois Freedom of Information Act (FOIA).

If, in response to this RFP, trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business responding to this RFP, such claim must be clearly made, and such information must be clearly identified. (5 ILCS 140/7 and 7.5) Responses to this RFP with every page marked as proprietary, privileged or confidential will not satisfy this requirement. Bidders are required to make a good faith attempt to properly identify only those portions of the response that are truly furnished under a claim that they are proprietary, privileged or confidential and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business responding to this RFP.

Redacted Version of RFP Response

In the event Responder believes and claims that certain materials or information contained in the submitted response are exempt from public disclosure under the Illinois FOIA, Responder is required to provide a redacted version of the response it believes will be suitable for release under the Illinois Freedom of Information Act. (5 ILCS 140/7 and 7.5)

A RESPONDER’S FAILURE TO PROVIDE A REDACTED VERSION OF THE RFP WILL RESULT IN SURS DISCLOSING THE RESPONDER’S ENTIRE RFP RESPONSE IF THE SAME IS REQUESTED UNDER THE ILLINOIS FOIA AND NEITHER THE RESPONDER NOR ANY THIRD PARTIES SHALL HAVE ANY RE COURSE AGAINST SURS FOR ITS DISCLOSURE OF THE NON-REDACTED RFP RESPONSE.

However, any claim of privilege from disclosure is not definitive. SURS has the right and legal obligation to determine whether such information is exempt from disclosure under the Illinois Freedom of Information Act and no information will be considered or determined by SURS to be proprietary, privileged or confidential unless it is identified and separated as indicated herein. (5 ILCS 140/7 and 7.5)

Ordinary Course of Business Communications Allowed

Other than existing normal business matters, respondents, potential respondents, or their representatives should not contact anyone at SURS (including SURS staff, members of the SURS advisory committees and members of the SURS Board) other than the listed RFP contact. In addition, respondents must not discuss this RFP with any employee of SURS, trustee of SURS, employee of SURS’ custodian, managers, legal counsel, or other advisors or persons/entities having contracts or other affiliations with SURS.
SURS Quiet Period Policy
Please note the following Quiet Period Policy establishing guidelines by which the SURS Board of Trustees and SURS Staff will communicate with prospective vendors or service providers during a search process. The Quiet Period for this RFP began on the date the RFP was issued: December 21, 2018.

1. The quiet period shall commence upon Committee action (or Board action if the selection is not initiated through a Committee) to authorize a search for a service provider and end once a selection has been made by the Board and accepted by the service provider;

2. Initiation, continuation and conclusion of the quiet period shall be publicly communicated via the SURS website (www.SURS.org) to prevent inadvertent violations;

3. All Board members, and SURS staff not directly involved in the search process, shall refrain from communicating with potential service providers regarding any product or service related to the search offered by the provider throughout the quiet period and shall refrain from accepting meals, travel, hotel, or other value from the providers;

4. Throughout the quiet period, if any Board member or SURS staff member is contacted by a potential service provider, the Board member or SURS staff member shall refer the provider to the SURS staff member directly involved in the search process;

5. All authority related to the search process shall be exercised solely by the relevant Committee or Board as a whole, and not by individual Board Members;

6. All information related to the search process shall be communicated by SURS staff to the relevant Committee or Board as a whole, and not to individual Board Members;

7. The quiet period does not prevent Board approved due diligence, client conference attendance, or communications with an existing service provider that happens to be a provider in the ordinary course of services provided by such service provider; however, discussions related to the pending selection shall be avoided during those activities;

8. The provisions of this policy will apply to potential service providers throughout the quiet period and shall be communicated to providers in conjunction with any competitive proposal process; and

9. A potential service provider or vendor may be disqualified from a search process for a violation of the Quiet Period or any portion of this policy.

Rights Reserved
SURS reserves the right to amend any segment of the RFP prior to the announcement of a selected vendor/contractor. In such an event, all respondents will be afforded the opportunity to revise their proposals to accommodate the RFP amendment.

SURS reserves the right to remove any or all services from consideration for this contract. At its discretion, SURS may issue a separate contract for any service or groups of services included in this RFP. SURS may negotiate additional provisions to the contract awarded pursuant to this RFP.

SURS may request additional information from any or all bidders to assist in the evaluation of proposals, and SURS reserves the right to conduct background investigations of selected individuals or firms prior to awarding a contract under this RFP.

SURS does not bear any obligation to complete the RFP process or to select any individual(s) or firm(s). SURS also reserves the right without prejudice to reject any or all proposals submitted.

SURS will NOT reimburse any expenses incurred in responding to this RFP.
Equal Opportunity
SURS does not discriminate because of race, color, religion, creed, sex, sexual orientation, age, marital status, military status, certain unfavorable discharges from military service, political affiliation, citizenship, ancestry, national origin, physical or mental handicap or disability or any other characteristic protected by law. It is the System’s intent to comply with all state, federal, and local equal employment and opportunity laws and public policies.

Terms and Conditions
Following a review of submitted materials, if requested, selected individuals or organizations must be prepared to make a presentation or otherwise participate in an in-person interview in Champaign, IL or in Chicago, IL with SURS staff members and/or members of the SURS board of trustees at a date and location to be determined by SURS. SURS will not provide reimbursement for any costs incurred by the individuals or organizations associated with this presentation. Prior to the award of a contract pursuant to this RFP, selected individuals or firms must provide all requested documentation.

Appendix A: Statement of Minimum Qualifications

(Firm Name) __________________________________________ certifies that it meets the following minimum qualifications.

Please initial each as applicable.

1. _______ The responder’s key professionals and/or organization has no material conflicts with the SURS Board.
2. _______ A minimum of 5 years in business providing Managed Security Services.
3. _______ Must maintain a staff of certified security professionals that are available 24/7/365.

Signed: ___________________________ Date: ___________________________

Title: ___________________________
Appendix B: Questionnaire

The following questionnaire must be completed and included with your response to this RFP. Type your responses in the same order as the questionnaire, listing the question first followed by your answer.

Contact and Company Information:

Name of Individual / Organization: ________________________________
Mailing Address: ________________________________

City: __________________ State: ______ Zip Code: _____ Phone: _____
Fax: __________________

Federal Employer Identification Number: ___________________________

Contact Person(s):
Name: __________________ Phone: __________________ Title: ____________

Fax: __________________ Email: __________________ Website: ____________

Organization Background:

1. Please provide a general description and history of the organization, its operations (please include any history of mergers and/or acquisitions), year founded, ownership structure, biographies of the principals and percentage ownership by current employees.

2. Provide a brief, descriptive statement detailing evidence of the respondent’s ability to deliver the goods or services sought under this RFP.

3. Is Respondent a “Minority owned business,” meaning a business which is at least 51% owned by one or more minority persons, or in the case of a corporation, at least 51% of the stock in which is owned by one or more minority persons; and the management and daily business operations of which are controlled by one or more of the minority individuals who own it? If so, please provide a detailed explanation.

4. Is Respondent a “Female owned business,” meaning a business which is at least 51% owned by one or more females, or, in the case of a corporation, at least 51% of the stock in which is owned by one or more females; and the management and daily business operations of which are controlled by one or more of the females who own it? If so, please provide a detailed explanation.

5. Is Respondent a “Business owned by a person with a disability,” meaning a business that is at least 51% owned by one or more persons with a disability and the management and daily business operations of which are
controlled by one or more of the persons with disabilities who own it? A not-for-profit agency for persons with disabilities that is exempt from taxation under Section 501 of the Internal Revenue Code of 1986 is also considered a "business owned by a person with a disability". If so, please provide a detailed explanation.
Appendix C: Fee Proposal

Please include detail regarding scope and cost of services, deliverables and timeframe for completion of the project.

FIRM NAME: _______________________________________________________

ADDRESS: _______________________________________________________

____________________________________________________________________

TELEPHONE: _______________________________________________________

REPRESENTATIVE: ___________________________________________________

1. Services as noted in Appendix E
   a. Threat Monitoring
   b. SIEM
   c. Threat Protection
   d. Firewall Management

2. Incident Response and Forensic Services, if available

3. Please include details for any of your Security Operations Centers that could accommodate a site visit

4. Please list 3 reference contacts, public sector experience preferred

5. If applicable, describe any additional ways to differentiate your company from other companies in providing services requested under this RFP, including any additional value-added goods and/or services that can be provided. If practical, the costs associated with any such value-added goods and / or services shall be included in the Proposal as a separate cost. Proponent should also state any opportunities that provide additional immediate or subsequent future savings from efficiencies gained through a proposed value added good or service.

Indicate project duration and frequency of visits below.

____________________________________________________________________

____________________________________________________________________
TOTAL Time & Materials NOT TO EXCEED Amount: $______________________________

Cost for additional meetings, if requested by SURS: $______________________________

I, _________________________________________, an authorized representative of the above-indicated firm, have reviewed and understand the ______________________ Request for Proposals, and I/we am/are prepared to provide the required services for the above costs.

__________________________________
(SEAL)

ATTACH A MINIMUM OF TWO PROJECT REFERENCES, SIMILAR IN DESIGN AND SCOPE.

ATTACH LIMITS OF COVERAGE FOR PROFESSIONAL LIABILITY INSURANCE.
Appendix D: Addendum to Contract

ADDENDUM TO CONTRACT

In consideration of SURS entering into such contract, the Vendor/Contractor also agrees to the following:

1) If the Contractor is an individual, he or she certifies that he or she is not in default on an educational loan as provided in Section 3 of the Educational Loan Default Act, 5 ILCS 385/3.

2) The Contractor certifies that it is not barred from being awarded a contract or subcontract because of a conviction or admission of guilt for bribery or for bribing an officer or employee of the State of Illinois or any other state in that officer or employee’s official capacity as provided in Section 50-5 of the Illinois Procurement Code, 30 ILCS 500/50-5.

3) The Contractor certifies that it will provide a drug free workplace by engaging in the conduct prescribed in Section 3 of the Drug Free Workplace Act, 30 ILCS 580/3.

4) The Contractor certifies that it is not barred from contracting with SURS because of a violation of either Section 33E-3 (bid-rigging) or 33E-4 (bid rotating) of Article 33E of the Criminal Code of 1961, 720 ILCS 5/33E.

5) The Contractor certifies that neither it nor any substantially owned affiliated company is participating or shall participate in an international boycott in violation of the provisions of the U.S. Export Administration Act of 1979 or the regulations of the U.S. Department of Commerce promulgated under that Act.

6) The Contractor certifies that no fees, commissions, or payments of any type have been or will be paid to any third party in connection with the contract to which this is an addendum, except as disclosed in the contract or an exhibit thereto as provided in 30 ILCS 500/50-25 and in 40 ILCS 5/1-145. The Contractor shall promptly notify SURS if it ever has reason to believe that this certification is no longer accurate.

7) To the extent Illinois law is applicable to Contractor, pursuant to 775 ILCS 5/2-105, Contractor agrees to:
   a) Refrain from unlawful discrimination and discrimination based on citizenship status in employment and undertake affirmative action to assure equality of employment opportunity and eliminate the effects of past discrimination;
   b) Comply with the procedures and requirements of the Illinois Department of Human Rights’ regulations concerning equal employment opportunities and affirmative action;
   c) Provide such information, with respect to its employees and applications for employment, and assistance as the Illinois Department of Human Rights may reasonably request; and
   d) Have written sexual harassment policies that shall include, at a minimum, the following information:
      i) The illegality of sexual harassment;
      ii) The definition of sexual harassment under State law;
iii) A description of sexual harassment, utilizing examples;

iv) Contractor’s internal complaint process including penalties;


vi) Directions on how to contact the Illinois Department of Human Rights and the Illinois Human Rights Commission; and

vii) Protection against retaliation as provided by Section 6-101 of the Illinois Human Rights Act. A copy of the policies shall be provided to the Illinois Department of Human Rights upon request.

8) To the extent it applies to Contractor and this contract, Contractor agrees to comply with the Illinois Prevailing Wage Act, 820 ILCS 130/1, et seq.

9) Contractor shall maintain, for a minimum of five (5) years after the completion of the contract, adequate books, records, and supporting documents to verify the amounts, recipients, and uses of all disbursements of funds passing in conjunction with the contract. Contractor shall further make all such books, records, and supporting documents related to the contract available for review and audit by the internal auditor of SURS and by the Illinois Auditor General and shall cooperate fully with any audit conducted by the internal auditor of SURS and the Illinois Auditor General and will further provide the internal auditor of SURS and the Illinois Auditor General full access to all relevant materials.

10) Contractor agrees to notify the SURS Ethics Officer if it solicits or intends to solicit for employment any of the employees of SURS during the term of the contract.

11) Contractor understands that SURS and this contract are subject to the provisions of the Illinois Open Meetings Act (5 ILCS 120/1, et seq) and the Illinois Freedom of Information Act (5 ILCS 140/1, et seq).

12) Counterparts. This Agreement and Addendum may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. The counterparts of this Agreement and Addendum may be executed and delivered by facsimile or other electronic signature by any of the parties to any other party and the receiving party may rely on the receipt of such document so executed and delivered by facsimile or other electronic means as if the original had been received.

Under penalties of perjury, Contractor certifies that ________________________________ is its correct Federal Taxpayer Identification Number.

Contractor is doing business as a(n) (please circle applicable entity):

- Individual
- Corporation
- Sole Proprietorship
- Not-for-Profit Corporation
- Partnership
- Medical and Health Care Services Provider Corporation
- Real Estate Agent
- Governmental Entity
- Medical and Health Care Services Provider Corporation
- Tax Exempt Organization (IRC 501(a) only)
- Trust or Estate
- Other: ____________
Appendix E: Requirements

The State Universities Retirement System (SURS) is requesting proposals for Managed Services Solutions to acquire, implement and co-monitor a solution that provides Threat Monitoring & Cyber-Attack Defense, SIEM & Log Management, Incident Response & Event Investigation, Threat Protection and Vulnerability Management. Co-management of our firewall is a requirement. The ability to provide incident response services is also a consideration.

Threat Monitoring
- 24x7 Attack Monitoring / Event Monitoring / Mitigation in real-time
- Blocking of malicious activity
- 24x7 Logging of attacks and security events
- Call escalating for analysis, mitigation plan & implementation
- Alert on security violations, viruses, worms, malware and any other suspicious security activity
- Comprehensive reporting
- Monitoring, correlation and incident response

SIEM
- Collect and Correlate security events
- Access to 18 months of incident details
- Analyze and Store security events from networks, hosts, and critical applications
- Attack / Event analysis and recommendation for mitigation.

Incident Response
- Identify threats from log alerts, IDS/IPS, firewalls
- Contain the threat
- Security and compliance reporting
- Assist SURS in resolving reported security incidents
- Have available resources to help with the Eradication and Recover phase

Threat Protection
- Provide detection and protection against zero-day and targeted attacks, including advanced malware (trojan, virus, worm), APT (Advanced Persistent Threats)
- Recommendation for correlation rules to be provided on events across various logs of networks, systems, devices, applications etc.
- Timely notification and escalation of threats, anomalies and suspicious security events along with details of events and recommendation to mitigate the risk.

Firewall Management
- Device provisioning, deployment, upgrades and patch management
- Tuning and configuration management/co-management
- Event monitoring and analysis
- Maintenance, backup and recovery
- Backup and recovery
- Analysis and response to firewall security and health events
- Comprehensive reporting
Reporting and Dashboards
The vendors solution shall provide for compliance reporting, custom reporting and robust visibility through dashboards. Reporting should have capability of providing daily/weekly/monthly/quarterly/annual reports as necessary with the ability to easily run ad-hoc queries. Real-time analytics would be desirous.

Installation, implementation and configuration of required tools
Vendor shall implement and integrate the tools and include employee training.
Contents

1. Corporate Capabilities .............................................................................................................. 2
2. Qualifications and Staffing ........................................................................................................ 2
3. Implementation and Service Methodology ............................................................................... 2
4. Security Event Monitoring ......................................................................................................... 3
5. Security Device Management ................................................................................................... 4
6. Security Information Management ........................................................................................... 4
7. Advanced Analytics and Capabilities ........................................................................................ 5
8. Vulnerability Management Services ......................................................................................... 5
9. Incident Response .................................................................................................................... 6
10. Portals, Reports and Dashboards ............................................................................................. 6
11. Service Management ............................................................................................................... 7
12. Pricing and Contracts ............................................................................................................. 7
1. Corporate Capabilities
   1.1. Indicate the number of years your company has been in business.
   1.2. Indicate the number of years your company has offered the services in the MSS portfolio.
   1.3. Where is your company headquartered? Indicate how many security operation centers (SOCs) you have, and where each one is located.
   1.4. Describe all documented policies, procedures and audit requirements that will ensure maintaining the privacy and confidentiality of SURS’ data from the data of your other customers.
   1.5. Describe alliances with other companies you have that are related to your MSSs, such as using a third-party software as part of your MSS portfolio.
   1.6. Does your company subcontract MSS work to other third parties? If so, please list them, based on the services in scope, and describe your business relationship with each one.
   1.7. Please provide an overview of your plans for continuity of service to SURS.

2. Qualifications and Staffing
   2.1. Indicate how many MSS customers you have.
   2.2. Please provide a list of MSS customers in SURS’ industry or market sector. This should include three or more references of companies using your service that are of similar size to SURS.
   2.3. Indicate the total number of employees in your company, and the number of employees responsible for MSS delivery.
   2.4. Please describe the relative distributions of employees and SOCs in your MSS company, and how these are geographically distributed.
   2.5. What is the average employment time of an MSS analyst within your company?
   2.6. Describe the process for screening and hiring your MSS staff.
   2.7. Explain the process of initial and ongoing training of your security-monitoring staff.
   2.8. What is the ratio of monitored security devices to personnel? What is the ratio of managed security devices to personnel?
   2.9. Describe your customer support tiers, including the capabilities and location of staff at each tier.
   2.10. Indicate any industry certifications your security operation centers hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International Organization for Standardization (ISO) 27001. If so, please provide evidence.

3. Implementation and Service Methodology
   3.1. Provide a brief overview of your managed security services and any supporting products.
   3.2. Are your SOCs staffed 24/365? Describe your approach to supporting 24/365 remote security event monitoring and device/agent management.
3.3. Describe the architecture of your MSS delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs. Provide example architectural diagrams and descriptions. Indicate where there are any regional differences in architectures or technologies used. Finally, include and identify any elements that are delivered by third-party partners.

3.4. List the primary tools used to deliver your services. Describe the function or service offering they support, and indicate whether they are proprietary, commercial, or open source, for example, log collection, log management and storage, analytics, reporting, case management and workflow, and incident response.

3.5. Explain how these services, and any supporting products will use or interface with products SURS has in place for Firewall Management, Information Event Management, Log Monitoring, Vulnerability Management. Ensure that you include details on how you intend to connect to SURS' infrastructure to provide support.

3.6. Will your services require the use of proprietary technology that SURS must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements. Include any associated costs as a separate line item in your quote.

3.7. Explain how you use external data (e.g., threat intelligence feeds) to analyze potential threats to SURS' environment and describe what access to this data SURS will have.

3.8. Please provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and the methods of notification.

3.9. Indicate how your services will be delivered in our internal virtual (or cloud-based) infrastructure [identify virtualized infrastructure vendor products, if applicable]. Include details about how the services will accommodate the scaling (larger or smaller) of the virtual or cloud-based environment, the implications for technology deployment to support monitoring, and related contractual, license or cost implications.

3.10. Indicate how your services will be delivered in an external or public cloud infrastructure [identify specific infrastructure providers, if applicable]. Include technology and contractual or licensing requirements related to provisioning, ongoing monitoring and de-provisioning of services to the cloud infrastructure.

3.11. Explain infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.

3.12. Please provide an example of how your services detected and addressed a recent security incident.

3.13. Explain your methodology for detecting custom or targeted attacks directed at our users or systems.

4. **Security Event Monitoring**

4.1. Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), iSeries, Active Directory and vulnerability data.

4.2. Please describe the use of signature-based and correlation rules.
4.3. Explain your ability to analyze this data and to provide real-time event correlation between data sources, and real-time alerting of security incidents and system health incidents.

4.4. Explain how your company keeps signatures/rules updated.

4.5. Explain support for the creation and management of customized correlation rules. Explain the capabilities available to our staff for doing so. Describe any limitations, such as data sources, age and query frequency.

4.6. Explain your ability to analyze this data to identify when changes in behaviors of users or systems represents risk to our environment.

4.7. Explain your methodology for reducing false positives and false negatives and for classifying security-related events that represent a risk to SURS.

4.8. Describe how false positives are managed, and how your company will incorporate false positive feedback from SURS.

4.9. Describe the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts.

4.10. Indicate the level of interaction and support that our staff can expect from your security analysts to assess, investigate and respond to incidents.

5. Security Device Management

5.1. Indicate the capabilities of your services to manage our firewall.

5.2. Explain your process for updating software to include signature updates and system patches. How do you ensure that this is done in a nonintrusive manner to your customers?

5.3. For each management service, indicate your change management process and your willingness to modify to meet our requirements.

5.4. For device management services, indicate whether changes are reviewed to assess increased risk, exposure or the effects on capacity.

5.5. Describe the contractual and cost implications of changing devices from real-time monitoring to collection or reporting (or vice versa).

6. Security Information Management

6.1. Indicate the data sources supported for log collection, reporting and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent).

6.2. Will all raw event logs and data be collected and forwarded to your platform for storage? If no, describe the variation and options for full log event retention (if applicable).

6.3. Will our logs be compressed and encrypted in transit, and is it a guaranteed delivery via a store and forward type of solution? If so, please describe.

6.4. Will our logs be compressed and encrypted at rest? If so, please describe.
6.5. Indicate any limitations to your log collection capabilities, such as peak event rates, volume or sources.

6.6. Explain the capabilities that allow our staff to search and browse original log data. Describe any limitations to this capability.

6.7. Explain the capabilities of our staff to create and modify reports based on collected log data. Indicate any limitations, such as number of reports, complexity of queries and age of data.

6.8. Indicate your standard data retention policies and ability to modify them to meet our requirements.

6.9. Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available versus what is kept offline. If 366 days of storage is required, how will that be priced for SURS?

6.10. What is the process for adding additional log sources to the scope of service? Include the implications for deployment architecture, integration costs and ongoing costs.

7. Advanced Analytics and Capabilities

7.1. What technologies are used to enable advanced analytics?

7.2. Describe your use of predictive analytics, including specific approaches and models/algorithms used.

7.3. How do you profile and monitor entity and user activities and behaviors?

7.4. Describe any specific network monitoring and/or network forensics features, capabilities or offerings to detect advanced, targeted attacks.

7.5. Describe the data and threat visualization capabilities available to us via the portal.

7.6. Describe any managed detection and response-type service offerings (e.g., managed endpoint detection and response, threat hunting, remote response and containment).

8. Vulnerability Management Services

8.1. Describe the service capabilities to monitor vulnerability scans internally and externally with the organization.

8.2. Indicate the technologies used to conduct scans, both commercial and open source.

8.3. Provide details on your methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.

8.4. Describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan.

8.5. Describe integration capabilities with vulnerability assessment data, including how the vulnerability data is used in support of triaging and investigating potential security events, and alerting and reporting capabilities.

8.6. How can vulnerability scans be scheduled, initiated/managed via your MSS portal? How are results viewed in the portal?

8.7. Indicate what frequency your MSS can scan our environment.

8.8. How frequently is the vulnerability database updated, and what are the data sources used for that?
9. Incident Response

9.1. Are there any remote and/or on-site incident response (IR) activities included as part of the service? If so, describe the services provided, including specifics on what is included in the core services versus what is available as an additional service/offering.

9.2. Do you provide incident response activities, including breach response services, via an optional retainer? If so, describe the packages, service-level agreements (SLAs), costs and included services. Do you offer proactive services as part of a retainer? Which services are able to be delivered remotely (both proactive and reactive), and which require your staff to be physically on our site(s)?

9.3. Describe any self-service features for incident response provided via the portal (e.g., automated malware analysis, custom signature or correlation rule implementation).

10. Portals, Reports and Dashboards

10.1. Describe the information provided by and features available through the web-based portal or console associated with your services. Describe the underlying technology (HTML5, Flash, JavaScript, etc.) and minimum software.

10.2. Indicate whether all services and MSS features, including those delivered by partners, will be available via a single portal.

10.3. What authentication and identity management system does your portal support?

10.4. How does the portal provide us access to external threat intelligence feeds?

10.5. Can SURS access, and search log event data via your MSS portal?

10.6. Describe user roles available to us for your MSS portal (e.g., administration, view/report, etc.). Describe how user access to data and reports can be restricted based on role and group.

10.7. Describe any real-time chat/instant messaging and/or live video interaction available with your SOC staff.

10.8. Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)? Also, indicate if you provide single-direction or bidirectional support, and whether the integrations are subject to additional costs.

10.9. Describe the portal capabilities to enable our staff to create, update and close tickets.

10.10. Is there a smartphone/tablet application available? If so, briefly describe the supported platforms and functionality.

10.11. Describe operational, regulatory and executive reporting capabilities.

10.12. Indicate the number of predefined reports, including specific regulatory and compliance items supported, that will be available for SURS. Please provide examples.

10.13. Explain the capabilities for our staff to create customized, ad hoc queries and reports. Describe any limitations to ad hoc query or report generation, including data sources, data age and query frequency.

10.14. Explain how report data can be exported to or used by an external report writer or risk dashboard.
11. Service Management

11.1. Explain the expected working relationship, roles and responsibilities between your security staff and Surs' security staff.

11.2. Indicate device/agent management, and real-time event management notification service levels. Explain how they are measured, and how they will be communicated to Surs.

11.3. Describe your problem resolution and escalation procedure.

11.4. Describe your SLA performance reporting.

11.5. Does your company have standard time frames, after which a given security product is no longer supported? If so, please describe the details, including proprietary and third-party software time frames.

11.6. Please provide details on support agreements. If a third-party software update is required, when does the SLA between you and Surs begin?

11.7. Describe the process for adding services or new technologies. For example, assume that Surs adopted a deep-packet-inspection firewall technology — how would this be supported and incorporated into an SLA?

11.8. What process will determine if a change is within the original scope of the supplied technology or a new feature? How will the costs be determined?

11.9. What access to internal-auditing documentation will you provide if our auditors, customers or business partners require this documentation in support of legal, regulatory or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit for producing documentation?

11.10. Describe the process should Surs have a complaint.

11.11. Indicate your process for notifying us of your noncompliance with the SLA.

11.12. Describe the remedies available to Surs should you fail to meet any SLAs.

11.13. Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSSP, if applicable?

11.14. Describe how Surs would obtain it's data during the separation process.

11.15. Describe how Surs' data (including data generated by your company about security events and incidents affecting Surs) will be governed and protected in transit. Consider this from a technology perspective, as well as via processes and procedures. How will the treatment of Surs' confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?

12. Pricing and Contracts

12.1. Please provide the name, title and appropriate contact information of the authorized negotiator or contract-signing agent.

12.2. Provide details on one-time costs and recurring costs.

12.3. Indicate and describe the licensing model(s) for your MSS offering.

12.4. Provide the base cost and pricing methodology.
12.5. Please indicate details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers) that are included in the cost.

12.6. How are costs negotiated for upgrading or expanding services? Can we add devices or data sources without affecting pricing or services?

12.7. How would the purchase of new security devices (or upgrading our current devices) affect pricing?

12.8. Provide any licensing and warranty information for third-party products you may require SURS to purchase in support of this service.

12.9. Indicate the discounts available, based on volume of services and contract length.

12.10. Will you allow SURS to test your service for a defined trial period?

12.11. Indicate any consulting support hours built into your standard MSS contracts.