REQUEST FOR PROPOSAL FOR
Network Penetration and Vulnerability Testing

Issued March 24, 2017

Responses due April 10, 2017 by 4:30 pm CST
Contents

I. Introduction .................................................................................................................................................. 3

II. Description of SURS .................................................................................................................................. 3

III. Services Required ....................................................................................................................................... 4

IV. Proposal Content ....................................................................................................................................... 5

   Cover Letter ................................................................................................................................................ 5
   Statement of Minimum Qualifications ........................................................................................................... 5
   Reference Checks ......................................................................................................................................... 5
   Questionnaire .............................................................................................................................................. 5
   Fee Proposal .............................................................................................................................................. 5
   Contract .................................................................................................................................................... 6

V. Submission of Proposals ............................................................................................................................ 6

VI. Evaluation Process .................................................................................................................................... 6

VII. Anticipated Timeline and Contact Information ..................................................................................... 7

   SURS Contact Information and Schedule: .................................................................................................. 7
   Submission Process .................................................................................................................................... 7

VIII. 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: ....................................................................................................................... 9
   Rights Reserved: ....................................................................................................................................... 10
   Equal Opportunity: ..................................................................................................................................... 10

Appendix A: Statement of Minimum Qualifications ..................................................................................... 12

Appendix B: Questionnaire ............................................................................................................................ 13

Appendix C: Fee Proposal .............................................................................................................................. 14
I. Introduction

SURS is seeking proposals from qualified candidates to conduct security assessments annually for three years. These assessments should give SURS a better understanding of potential vulnerabilities and risks that may be visible from the internet. Testing should be from the perspective of an outside attacker with no inside knowledge of the network.

External Network Penetration and Vulnerability Testing
Class C network, only up to 20 should be accessible to be penetration tested and scanned for vulnerabilities

External Web Application Security Assessment
4 applications, only 1 done per year
Up to 4 roles
100 Dynamic Pages

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 for 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 220,000 members (approximately 163,000 active and inactive, as well as 57,000 annuitants) who work for 65 employers. SURS is responsible for investing assets of more than $15 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 $1.3 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”.
SURS currently employs approximately 120 staff, located in 2 offices in Champaign and Naperville, Illinois. Two SURS employees are located in the Naperville office. The remainder of SURS employees is 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. The Act also encourages the Board to increase the racial, ethnic, and gender diversity of its fiduciaries, to the greatest extent feasible within the bounds of financial and fiduciary prudence. In furtherance of this Act, SURS will use its best efforts to increase the racial, ethnic, and gender diversity of its vendors/investment managers.

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 investment managers or other service providers. However, each investment manager or service provider should be familiar with the provisions of this section and comply with this section if the investment manager or service provider deems it appropriate.

III. Services Required

External Network Penetration and Vulnerability Testing

- Testing of identified IP addresses to attempt to gain access.
- Broad scans to identify potential areas of exposure and services that may act as entry points.
- Identification of vulnerabilities.
- Targeted scans and manual investigation to validate vulnerabilities.
- Identification of issues of immediate consequence and recommended solutions.
- Ranking of vulnerabilities based up on threat level, loss potential and likelihood of exploitation.

External Web Application Security Assessment

- Dynamic vulnerability scanning.
- Malicious code analysis.
- Manual code review.
- Manual penetration testing.
- Project Management
  Monitor and control project and ensure that it is completed in satisfactory and timely manner.

---

1 Note: While SURS is not subject to the Illinois Procurement Code generally (30 ILCS 500/1-15.100), each responder should comply with any applicable sections of the Illinois Procurement Code.
IV. 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 in a separate section. The proposal should include a table of contents. Failure to provide information in the prescribed format may result in rejection of the proposal. All responses will be subject to verification for accuracy. **Proposals containing false or misleading information will be rejected.**

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 may be conducted for each finalist.

Questionnaire

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

Fee Proposal

Proposers must submit their fee in the format prescribed in Appendix C. Any deviation from the
prescribed format which in the opinion of SURS is material may result in the rejection of the proposal. The proposed fee shall include all costs and expenses for providing the services to SURS as described in this RFP. 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.

V. 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.

Subject must contain “Response to Request for Proposals for Network Penetration and Vulnerability Testing.” Failure to clearly identify the proposal in the subject line may result in the rejection of the proposal. SURS is not responsible for receipt of any proposal which is improperly labeled.

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.

VI. 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

Proposals that pass the pre-evaluation review will undergo an evaluation process conducted by SURS
staff. SURS will consider the following various elements in the decision process, ranked in no specific order, and will render a decision based on the perceived 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
- Soundness of the approach and quality of the proposed services
- Firm qualifications including established record of success in similar work
- Individual qualifications of the assigned staff
- Proposed deliverables
- Cost

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.

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

VII. Anticipated Timeline and Contact Information

SURS Contact Information and Schedule:

Byron Campbell
bcampbell@surs.org
SURS
1901 FOX DR
PO BOX 2710
CHAMPAIGN, IL 61825-2710

Date RFP Issued March 24, 2017
Deadline for Submitting RFP Response April 10, 2017
Proposal Evaluation April 10, 2017– April 14, 2017
Consultant(s) Selected April 14, 2017

Submission Process
Deadline:
To be considered for selection, proposals must be received via e-mail in Adobe Acrobat format by Mr. Byron Campbell at bcampbell@surs.org no later than 4:30 p.m. CST, April 10, 2017. Please reference the “Network Penetration and Vulnerability Testing RFP Response – Name of Responder” in your communications. An e-mail 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 vendor and received by Mr. Byron Campbell at

---

2 *All dates are subject to change at SURS discretion*
bcampbell@surs.org no later than the deadline of 4:30 p.m. CST, April 10, 2017. Please reference the “Network Penetration and Vulnerability Testing RFP Response - Name of Responder” in your communications. An e-mail 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 maintain the integrity of the RFP process, interested proposers are expected to respond to this RFP to the best of their knowledge without asking questions or requesting clarification. If a proposer discovers an error or has a question regarding the RFP, the proposer should notify the SURS contact person listed in the previous section, in writing. SURS will respond only to questions that are presented in writing via e-mail to: Mr. Byron Campbell at bcampbell@surs.org. All questions should be submitted to SURS by 4:30 p.m. CST, April 4, 2017. These questions will be consolidated into a single Q&A document and responded to by SURS on, or about, April 6, 2017. The Q&A document will be posted on the SURS web site at www.surs.org/rfp without indicating the source of the query. If deemed necessary or appropriate in the System’s discretion, SURS may clarify or modify any part of this RFP by posting notice on the SURS website prior to the proposal deadline.

Proposal Evaluation
All proposals received by the SURS representative, Mr. Byron Campbell, by the deadline of 4:30 p.m. CST, on April 10, 2017 will be reviewed to determine whether they meet the requirements of this RFP.

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.
VIII. 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 certain materials in the submitted response are exempt from public disclosure in accordance with language in Section V FOIA Disclosure, Responders are asked 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)

However, any claim of privilege from disclosure is not definitive. SURS has the right and legal obligation to determine whether such information is exempt form 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 individual assigned to the RFP listed above.

In addition, respondents must not discuss this RFP with any employee of SURS's 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 March 23, 2017.
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 this policy.

Rights Reserved:
SURS reserves the right to amend any segment of the RFP prior to the announcement of a 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 of the 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.
Appendix A: Statement of Minimum Qualifications

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

Please initial each as applicable.

1. _____ Stated firm/individual has a minimum of five years’ experience providing Penetration Testing and Web Application Assessments.

2. _____ Stated firm/individual will have certified personnel preforming Penetration Testing and Web Application Assessments.

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 Firm: ________________________________________________________________
Mailing Address: _______________________________________________________________
City: __________________________ State: _________ Zip Code: ______________________
Phone: ____________________ Fax: _____________________________________

Federal Employer Identification Number: ________________________________________

Contact Person(s):
Name: ____________________________ Phone: _____________________________
Title: _____________________________ Fax: _______________________________
Email: __________________________ Website: ___________________________

Firm Background

1. Please provide a general description and history of the firm, 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. Briefly describe your firm’s background and history of performing Penetration Testing and Web Application Assessments.

3. How many IT professionals are employed by your firm and what is their level of experience? Please list the firm’s professional staff that you perceive to be assigned to this engagement, their professional credentials, and an estimated timeframe for completion.

4. Describe the turnover of the firm over the past five years.

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

Client Relationships

1. Please provide three references (preferably one from a public pension fund client) from IT engagements that you/your firm have conducted in the last two years. By providing references, the proposer authorizes SURS to contact the reference to inquire about the proposer’s services.
Appendix C: Fee Proposal

Please quote your flat fee for the following items. Please detail the scope of services to be provided under the proposed engagement and provide quotes for any additional services.

A. Services $__________
B. Estimated Expenses $__________