1 NOTICE TO BIDDERS

1.1 Notice

The Board of Trustees of the Nebraska State Colleges will receive responses to a Request for Proposal (RFP) in the form of sealed bids for a one-year contract with four optional one-year extensions for Operational Cybersecurity Staff Augmentation Services (OCSAS) for its three member schools: Peru State College (PSC), Chadron State College (CSC), and Wayne State College (WSC), as well as for the System Office itself. Bids will be received via email to ocsasrfp@nscs.edu until 4:00 p.m. CDT on October 1, 2021, at which time and place the bids will be publicly opened. Emails should have the subject line "NSCS OCSAS RFP Response".

1.2 Basis of Bid Proposals

Bid proposals are to be based upon specifications contained in the Request for Proposals for OCSAS, including all sections. No telephone or fax proposals will be considered. No bidder may withdraw a bid for a period of one hundred (100) days after the date of bid opening.

1.3 Contractor Selection

The Bidders will be screened and a Contractor selected on the basis of any and all information that the College deems pertinent to the solution. The NSCS reserves the right to reject any or all proposals, to accept other than the low bid, to negotiate with one or more bidders on the basis of their initial proposal, and to waive informalities or technicalities in the bidding and evaluation process.

1.4 Disclosure requirements

Contracts executed as a result of this RFP are subject to statutory public disclosure and public website posting requirements. Information submitted with your bid proposal and written responses is subject to disclosure requirements under the Nebraska Public Record statutes. Information may only be withheld from the public under very limited circumstances. Documents submitted as part of the bid proposal containing trade secret or proprietary information must be submitted in supplemental documents clearly marked "Proprietary."

1.5 Contract and Contract Documents

The NSCS and the successful respondent shall enter into a written contract.

2 SELECTION PROCESS AND CRITICAL DATES

The following summary outlines the steps to be followed in the process of selecting a contractor and the critical dates established for each step.

- Request for Proposal Issued Sept 10, 2021
  - Specifications, including the calendar of events, bidder's qualification requirements, notice of mandatory pre-proposal conference and other information, are issued to prospective Contractors.
- Mandatory pre-bid meeting Sept 27, 2021 (10AM CDT)
  - A mandatory pre-bid environment discussion will be held for interested vendors to tune responses to the Entity environments. This will also be a venue for Q&A.
  - https://wsc.zoom.us/j/93709032044?pwd=NHQvVVFtYTFEbVdnOS81Lzl5ay9NQT09

- Proposal Due Date October 1, 2021
  - Proposals submitted in response to this Request for Proposal must be received by 4:00 p.m. CDT on Friday, October 1, 2021.
- Finalist Presentations October 11-15, 2021
  - During this period, the committee may request that selected prospective Contractors make virtual presentations on their proposals.
- Selection of Finalist October 18, 2021
  - The review and evaluation committee and appropriate campus officials will evaluate all responsive proposals in accordance with the review and evaluation procedures outlined in the Request for Proposal.
- Contract Negotiations Complete October 29, 2021
  - Contract is completed and submitted to the Board of Trustees for review.

3 INSTRUCTIONS TO BIDDERS

3.1 Communication

Communication with members of the RFP committee or members of the campus community on matters relating to this RFP must be done during designated conference meetings or presentations as outlined by this RFP or via e-mail:

- To: OCSASRFP@nscs.edu
- Subject line: NSCS OCSAS RFP Questions

Communication outside this protocol may be grounds for elimination for consideration.

3.2 Proposal Submission

Proposals shall be submitted via e-mail to ocsasrfp.wsc.edu with the subject line "NSCS OCSAS RFP Response." Proposals should conform to the format provided at the end of this RFP. Format compliance will be considered in the evaluative process as an indicator of the respondent's willingness to collaborate with the NSCS.

3.3 Proposal Review and Evaluation Committee

Proposals submitted in response to this RFP shall be reviewed and evaluated by a committee of IT professionals and administrators from the NSCS System Office and IT offices at each campus:

- NSCS System Office Vice Chancellor for Facilities and IT
- NSCS Chief Information Officer
- Chadron State College CIO/CISO
- Peru State College CIO/CISO
- Wayne State College CIO/CISO
- Up to two IT staff from each campus

3.4 Campus Interviews

Selected bidders may be invited to make virtual presentations for the purpose of clarifying proposals.

3.5 Proposal Evaluation Methodology

The committee will score proposals based on the following criteria:

Essential Services provided	30%
Additional Service provided	3%
Integration plan with existing IT staff	10%
Service Level Agreement	10%
References	5%
Qualifications of personnel	5%
Quality of RFP Response	5%
Ease of Contract Negotiation	2%
Overall economic value of the proposal	30%

4 GOALS, DEFINITIONS, AND ESSENTIAL SERVICES

Section 4 outlines the goals of the RFP, definitions of specific terms, and minimum technical services required by the NSCS for responses to be considered for evaluation. Respondents must describe their ability to provide these services in Section 6.

4.1 Goals

The NSCS seeks to improve their cybersecurity posture and decrease both the impact and likelihood of cybersecurity incidents at all three Colleges and the System Office. The NSCS seeks to accomplish this by:

1. Augmenting existing staff cybersecurity efforts with managed security services,
2. Improve alignment with NIST 800-171 by closing gaps in compliance with NSCS IT Security Standards
3. Implement controls recommended by insurance carriers across the system to improve security and control insurance costs
4. Develop the cyber security skills of existing IT Staff
5. Enhance collaborative efforts across the System
6. Advise on consistent tools/mechanisms for security controls across the System

4.2 Definitions

Entity – Any of the three Colleges or the System Office itself. If an entity has multiple physical locations, those locations are also included in the entity.

IT Staff – Staff directly employed by an Entity for IT work or contracted by the Entity to provide IT managed services.

Service – the aggregate collection of Operational Security Services and Integration with IT Staff

NSCS IT Security Standards – The NSCS IT Security Standards framework – available at: https://www.nscs.edu/information-for/employees/isp-standards

IR – Incident Response

4.3 Essential Security Services

The successful respondent will provide all the services identified in this Section as a part of their basic response. While other services may be provided as optional components with additional fees, these services are required.

4.3.1 Prevention

4.3.1.1 Phishing Campaigns

The successful respondent will plan, orchestrate, and score internal phishing campaigns as well as work with each Entity to integrate scoring into user security awareness training requirements. The respondent will provide a platform to deliver said campaigns or, at the discretion of the Entity, work with a College provided platform to deliver campaigns.

4.3.1.2 User Security Awareness Training (Including PCI-DSS)

The successful respondent will provide user security awareness training sessions as determined by the Entity CISO to supplement training resources already available. Such training may be tailored to specific cyber security topics such as PCI-DSS.

4.3.2 Protection

4.3.2.1 Perimeter Monitoring

The successful respondent will actively monitor the network perimeter for each Entity's sites, notify the Entity of potential vulnerabilities. This service is not a full formal penetration testing program for audit compliance, etc. but rather is intended to assist the Entities in rapidly identifying and resolving vulnerabilities.

4.3.2.2 Vulnerability Assessment

The successful respondent will, no less frequently than semi-annually, provide a vulnerability assessment, including: on-premise perimeter, on-premise internal, public cloud, and private cloud services.

4.3.2.3 Threat & Log Monitoring

The successful respondent will actively monitor threats and logs, providing 24/7 notification to Entity IT Staff and pre-coordinated remediation where possible. The successful respondent will utilize integrated event dashboards such as Palo Alto's Cortex/XDR and/or Microsoft 365 Defender. As part of this service, successful respondents will also provide a hosted Security Incident and Event Management (SIEM) platform scoped for satisfying the requirements of the Service.

4.3.2.4 Threat Hunting

The successful respondent will proactively search each Entity's network for active threats and, where appropriate, provide immediate remediation in alignment with decision frameworks pre-agreed upon with the Entity CISO.

4.3.2.5 Suspicious email/file review

The successful respondent will provide real-time review of e-mail and file storage patterns and alert IT Staff of suspicious patterns or, where appropriate, provide immediate remediation in alignment with decision frameworks pre-agreed upon with the Entity CISO.

4.3.3 Mitigation

4.3.3.1 Mitigation Research & Implementation Plan

The successful respondent will aggregate and analyze data gathered from other OSS Protection services such as Threat Hunting, Vulnerability Assessment, gaps with NSCS IT Security Standard compliance, and industry research and no less than monthly, create or update an implementation plan for mitigation controls. In the event of specific threats requiring immediate intervention, the successful respondent

will adjust the Implementation Plan and work with IT Staff to implement mitigations as a real-time response.

4.3.3.2 Security Product/Controls Configuration & Management

The successful respondent will provide guidance and assistance to IT Staff in configuration and management of security products and controls, including, but not limited to: Microsoft 365 Defender/ATP, Palo Alto Strata, Cortex, and XDR, Aruba ClearPass, Fortinet firewall products, and Cisco firewall products to fulfill the Mitigation Implementation Plan.

4.3.4 Response

4.3.4.1 Incident Response (Technical and Lead)

The successful respondent will, in the event of an incident, provide initial Incident Response (IR) until such time as an IR resource is assigned and engaged through the Entity's Cyber Insurance provider. The successful respondent will partner in knowledge transfer and hand-off to the ongoing IR provider as needed.

4.4 IT Staff Integration

4.4.1 Knowledge Transfer

The successful respondent will partner with IT Staff for regular knowledge transfer with the goal of providing cyber security focused professional development for IT Staff who are directly employed by each Entity.

4.4.2 Collaboration Leadership

The successful respondent will partner with the Entity CISOs to identify opportunities for Entity IT Staff to collaborate in implementing best practices on common or disparate security platforms, including regular coordination meetings with the Entity CISOs and invited staff.

4.4.3 Change Control

The successful respondent will work with the Entity CISO to identify and utilize a change control framework that facilitates:

4.4.3.1 Communication of planned changes for non-time sensitive or non-critical vulnerabilities

Example situation: A medium risk vulnerability is identified in Microsoft print services. The successful respondent communicates a mitigation recommendation for implementation by IT Staff during a weekly change window and then provides follow-up analysis to ensure the risk is remediated.

4.4.3.2 Immediate remediation of critical risks under pre-arranged conditions

Example situation: A remote-desktop port is found open on a perimeter scan. Because RDP is a service that has been listed as a 'never publicly available' service, the successful respondent implements a firewall change to remote access and communicates the change to IT Staff.

4.4.3.3 Immediate communication and planning for time-sensitive or critical risks that cannot be mitigated under pre-arranged conditions

Example situation: A non-authenticated privilege escalation vulnerability for Microsoft print services is announced over a weekend and the Entity utilizes Microsoft print services. The successful respondent will contact IT Staff during off-hours and coordinate an appropriate mitigation.

4.4.4 Reporting

The successful respondent shall provide a plan for monthly reporting of cybersecurity posture for each Entity and for the NSCS in summary, including relative risk change. The successful respondent shall also provide an annual report of mitigations and controls successfully implemented at all Entities to provide the NSCS staff with negotiating tools to help contain cybersecurity insurance costs.

5 GENERAL CONDITIONS

The terms in Section 5 will be included in the final Contract. Respondents must indicate their willingness to accept these terms in Section 6.

5.1 Prompt Payment Act.

In the event any amount due under this Contract remains unpaid for forty-five (45) days after the due date, the unpaid amount shall bear interest from the 31st day after the due date at the rate specified in the Prompt Payment Act, Neb. Rev. Stat. §§81-2401 to 81-2408.

5.2 Independent Contractor.

The Contractor shall be an independent contractor and not a College employee for all purposes, including, but not limited to, the application of the Fair Labor Standards Act, minimum wage and overtime payments, the Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code, any Nebraska revenue and taxation law, Nebraska workers' compensation law and Nebraska unemployment insurance law.

5.3 Independent Enterprise.

The Contractor agrees that it is a separate and independent enterprise from the College, that it has a full opportunity to find other business, that it has made its own investment in its business, and that it shall utilize a high level of skill necessary to perform the work. This Contract shall not be construed as creating any partnership, joint venture, or joint employment relationship between the Contractor and the College, and the College shall not be liable for any obligation incurred by the Contractor, including but not limited to unpaid minimum wages or overtime premiums. If the Contractor has employees or subcontractors, the Contractor further agrees to maintain at least the prescribed minimum workers' compensation insurance coverage for all of the Contractor's employees for the duration of this Contract. The Contractor agrees to furnish the College proof of workers' compensation insurance coverage upon request.

5.4 Liability Insurance Requirements.

The Contractor is required to carry liability insurance in the amount of one million dollars ($1,000,000) per occurrence. The Contractor's insurance policy shall be primary and non-contributory. The College shall be named as an additional insured party on the policy and the certificate of insurance shall reflect that the policy waives its right of subrogation against the College. A copy of the certificate shall be provided to the College.

5.5 Access to Records.

The Contractor agrees to maintain complete records regarding the expenditures of funds provided by the College under this Contract. The Contractor agrees to allow authorized representatives of the College, the Board, the funding Federal Agency, if any, and the United States Comptroller General, if appropriate, free access at reasonable times to all records generated or maintained as a result of this Contract for a period of three (3) years after the termination of this Contract.

5.6 Employee Work Eligibility Status.

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of new employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of a newly hired employee.

The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the Contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

5.7 Non-Discrimination.

The Contractor agrees to comply fully with Title VI of the Civil Rights Act of 1964, as amended, the Nebraska Fair Employment Practice Act, Neb. Rev. Stat. §§48-1101 to 48-1125, as amended, and Board Policy 5000 in that there shall be no discrimination against any employee who is employed in the performance of this Contract, or against any applicant for such employment, because of age, color, national origin, race, religion, disability, sex, sexual orientation, or gender identity. This provision shall include, but not be limited to employment, promotion, demotion, transfer, recruitment, layoff, termination, rates of pay or other forms of compensation, and selection for training including apprenticeship. The Contractor further agrees to insert a similar provision in all subcontracts for services allowed under this Contract.

5.8 ADA & Drug-Free Workplace Requirements.

All provisions of this Contract are subject to the Americans with Disabilities Act (ADA). Further, the Contractor certifies that the Contractor operates a drug-free workplace and, during the term of this Contract, will be in compliance with the provisions of the Drug-Free Workplace Act of 1988.

5.9 Use of Information; Property Ownership.

The Contractor agrees that any and all information gathered in the performance of this Contract, either independently or through the College or the State College System, shall be held in the strictest confidence and shall be released to no one other than to the College, without prior written authorization of the College. The Contractor agrees that no authority or information gained through the existence of this Contract will be used to obtain financial gain for the Contractor, for any member of the Contractor's immediate family, or for any business with which the Contractor is associated except to the extent provided by this Contract.

The Contractor further agrees that any tangible or intangible property, including patents, trademarks and other intellectual property, produced, developed, prepared, or created under the terms of this Contract shall be the property of the College. The Contractor hereby assigns and transfers to the College all right, title and interest in and to any copyright in any copyrightable materials produced under this Contract.

5.10 Parties; Subcontractors; Assignment.

References to the Contractor and the College include the parties' officers, employees, agents, and independent contractors and subcontractors. The Contractor agrees that no subcontractors shall be utilized in the performance of this Contract without the prior written authorization of the College. The

Contractor agrees not to assign or transfer any interest, rights, or duties in this Contract to any person, firm, or corporation without prior written consent of the College.

5.11 Cancellation.

This Contract may be canceled by either party upon thirty (30) days' written notice. Settlement of the amount due to the Contractor upon cancellation shall be negotiated between the parties based upon (a) specified deliverables completed by the Contractor and accepted and usable by the College as of the date of termination when the Contractor initiates termination, or (b) the percentage of services performed by the Contractor as of the date of termination when the College initiates termination.

5.12 Default; Remedies.

If the Contractor defaults in its obligations under this Contract, the College may, at its discretion, exercise any remedy available by law or in equity. In addition to any other available remedy, the College may terminate this Contract immediately by written notice to the Contractor. The College shall pay the Contractor only for such performance as has been properly completed and is of use to the College. The College may, at its discretion, contract for provision of the services required to complete this Contract and hold the Contractor liable for all expenses incurred in such additional contract over and above the consideration set forth in Paragraph 3.

5.13 Unavailability of Funding.

Due to possible future reductions in state and/or federal appropriations, the College cannot guarantee the continued availability of funding for this Contract beyond the current fiscal year. In the event funds to finance this Contract become unavailable either in full or in part due to reductions in appropriations for a future fiscal year, the College may terminate the Contract or reduce the consideration by notice in writing to the Contractor. The notice shall be delivered by certified mail, return receipt requested, or in person with proof of delivery. The College shall be the final authority as to the availability of funds. The effective date of Contract termination or reduction in consideration shall be the actual effective date of the elimination or reduction of appropriations. In the event of a reduction in consideration, the Contractor may cancel this Contract as of the effective date of the proposed reduction by written notice to the College.

5.14 Complete Agreement; Governing Law; Amendment.

This Contract sets forth the entire agreement of the parties and supersedes all prior negotiations, discussions, and proposals. There are no promises, understandings, or agreements of any kind pertaining to this Contract other than those stated herein. This Contract will be construed, interpreted, governed and enforced under the laws of the State of Nebraska. This Contract may be amended at any time in writing upon the agreement and signature of both parties.

5.15 Technology Access.

All contracts that include provisions of technology products, systems, and services, including data, voice, and video technologies, as well as information dissemination methods, shall comply with the Nebraska Technology Access Standards adopted pursuant to Neb. Rev. Stat. §73-205. These Standards are available for viewing on the Web at http://nitc.ne.gov/standards/2-201.html, and are incorporated into this Contract as if fully set forth herein.

5.16 Confidentiality.

Contractor acknowledges that performance under the terms of this Contract may involve receipt of user data from the College. Contractor will utilize user data from the College only in the furtherance of this

Contract. Contractor will notify College within twenty-four (24) hours of becoming aware of any data breach of its systems which expose confidential College user data. Contractor will reimburse the College for any and all expenses incurred by the College as a result of a data breach of Contractor's systems.

If the user data consists of confidential student information protected by The Family Educational Rights and Privacy Act (FERPA) the Contractor agrees and acknowledges that Contractor is acting as an officer of the College for the purposes of this Contract as defined by Nebraska State College Board Policy 3650 (at the time of this writing available at: https://www.nscs.edu/directory_record/45/3650_student_records) and will take necessary steps to safeguard the confidential student information.

The Contractor further acknowledges the obligation and agrees to comply with the General Data Protection Regulation (GDPR) privacy laws in regard to the collection, processing, storage, security, management, transfer and erasure of user data.

6 RESPONSE

The NSCS expectations and priorities for the OCSAS solution are defined on the next page Respondents are encouraged to use their expertise and creativity in crafting a response that addresses these expectations and priorities.

Responses must conform to the following format guide by tabulated section in paper format or section break in electronic format. Within this format, describe how the proposed solution will meet the Expectations of the College and how it will help to accomplish the College's Priorities.

6.1.1 Essential Services

Respondents must provide brief detail on how they would deliver each Essential Service.

6.1.1.1 Prevention

6.1.1.1.1 Phishing Campaigns

6.1.1.1.2 User Security Awareness Training (Including PCI-DSS)

6.1.1.2 Protection

6.1.1.2.1 Perimeter Monitoring

6.1.1.2.2 Vulnerability Assessment

6.1.1.2.3 Threat & Log Monitoring

6.1.1.2.4 Threat Hunting

6.1.1.2.5 Suspicious email/file review

6.1.1.3 Mitigation

6.1.1.3.1 Mitigation Research & Implementation Plan

6.1.1.3.2 Security Product/Controls Configuration & Management

6.1.1.4 Response

6.1.1.4.1 Incident Response (Technical and Lead)

6.1.2 Additional Services Provided

Respondents should detail any additional cybersecurity services they can provide in this section. This Section will be scored on the variety of additional services available and for potential future expansion, including relative cost to other similar proposals. Note that the overall calculation for cost will NOT include additional services costs.

6.1.3 IT Staff Integration

Respondents must provide a brief description of their plan for IT Staff Integration including, if available, examples of similar work with other institutions. If examples are provided, those institutions must be cited as references below.

6.1.3.1 Knowledge Transfer

6.1.3.2 Collaboration Leadership

6.1.3.3 Change Control

6.1.3.3.1 Communication of planned changes for non-time sensitive or non-critical vulnerabilities

6.1.3.3.2 Immediate remediation of critical risks under pre-arranged conditions

6.1.3.3.3 Immediate communication and planning for time-sensitive or critical risks that cannot be mitigated under pre-arranged conditions

6.1.4 Service Level Agreement

Respondents must indicate their maximum response times for the Essential Services by level of risk. For example:

- High: 2 hours
- Medium: 24 hours
- Low: 48 hours

Respondents must also indicate what framework they use to determine risk level. For example, risk levels are set by the NIST National Vulnerability Database version 3.1.

6.1.5 References

Respondents must provide at least 3 client references, including:

Contact name
Institution/organization name
Phone number
Email address

Ideally, references should be higher educations of similar size and scope to the Nebraska State College System and its Colleges.

6.1.6 Qualification of personnel

The respondent must provide the professional biography and certifications held by staff who would be assigned to work with the NSCS in fulfillment of the RFP.

6.1.7 Quality of RFP response

This item will be scored by the committee based on the degree to which the response follows the RFP format and provides the College with a compelling vision on how the Service will meet goals the of the RFP.

6.1.8 Contract ease of negotiation

6.1.8.1 For each clause in Section 5, indicate your acceptance of the contract language or propose an initial alternative for negotiation.

6.1.9 Overall economic value of the proposal

Provide the cost of the Essential Services and IT Staff Integration portions of the Solution. Student/Staff FTE counts and managed device counts are provided in Appendix A to assist respondents in appropriately pricing the Solution. The example items provided below are examples only. The Respondent should add or remove table rows as fits the cost of the Solution. Where optional costs are proposed, the Respondent should indicate clearly how the options interact with each other. Total economic value will take into consideration the total solution cost over the potential lifetime of the Contract (5 years). Example cost proposals are provided below:

NSCS cost proposal			
Item	**Basis of cost**	**One Time Cost**	**Annual Cost**
Initial Consultation	Flat rate per Entity	$10,000	--
Essential Services	Student+Staff FTE/year as measured by IPEDS	--	$8/FTE/year

OR			
Essential Services	Per managed device per year	--	$50/device/year
OR			
Essential Services	Other basis – provide detail	--	$Z
Additional Service X	Some basis of cost	--	$X
Additional Service Y	Some basis of cost	--	$Y

Attachment A

***IPEDS enrollment data

INSTITUTION	STUDENT FTE	STAFF FTE	TOTAL FTE
WSC	3230	408	3638
CSC	1874	297	2171
PSC	1546	198	1744
NSCS	0	17	17
Total	727	240	7570

Managed endpoint count data:

INSTITUTION	
WSC	1500
CSC	1175
PSC	725
NSCS	30
Total	3430