STATE OF NEW HAMPSHRIE
REQUEST FOR PROPOSALS
RFP ADDENDUM #1

RFP NUMBER AND TITLE:	RFP NHJB-2023-05 Information Security Audit
AMENDMENT DATE:	June 16, 2023
PROPOSAL DUE DATE:	June 30, 2023
RFP ISSUED BY:	State of New Hampshire Judicial Branch Administrative Office of the Courts
Unless specifically addressed below, all other provisions and clauses of the RFP remain unchanged.	

Provided below are submitted written questions received and the NHJB's answers

Question #	Question	Answer
1.	Can offshore personnel (outside the United States) work on this project?	No, all personnel must be able to legally work in the United States and pass a criminal records background check.
2.	Is there a budget for this project? What is the budget estimate?	Yes, there is a budget for this project. The budget estimate will not be shared publicly.
3.	Please describe the frequency of onsite visits?	To be determined during the course of the work. On-site work is not required unless portions of the audit require an individual to be physically present to access systems not available remotely. This may require 4 days annually on-site.
4.	Is there a preference for a company with DVBE, SB, MVE etc. certifications?	The team should consist of individual contributors that have certifications with the products NHJB uses, Microsoft and Cisco. Section IV.B.1. e & f of the RFP
5.	Is there a template to use for cost proposal? Should cost proposal be submitted separately?	There is no template. Yes, the cost proposal should be separate from the technical proposal. However, it should be submitted in the same email.
6.	Did NHJB receive 3rd party assistance in preparing this RFP?	No.

7.	What are the most important expectations you have for a security partner?	Delivering more than just findings. Work as an extension of the IT Department with a focus on knowledge transfer and assistance with remediation where appropriate.
8.	What are your top requirements for the solution provider you choose which will set them apart from other bidders?	Experience of the individual contributors on the team, cost, thoroughness of proposal, and references.
9.	What are the top three outcomes you are looking for?	Better understanding of overall security posture, prioritized actionable steps, NHJB IT staff coming away from the audit with increased knowledge/understanding of security standards and best practices and their applicability to the NHJB environment.
10.	How is success defined for this project?	Completion of RFP Section IV.A. & B.
11.	Who are the key stakeholders for this project?	NHJB IT Department and NHJB senior leadership.
12.	Are wet signatures required, or will digital signatures suffice?	Digital signatures on the proposals may be accepted.
13.	May we submit a redacted copy of our response for public inspection under the Freedom of Information Act ("FOIA")?	Yes. See RFP Section VIII, E.
14.	Will the NHJB be able to guarantee the confidentiality of the complete and unedited customer list if it is properly marked as confidential?	No. See RFP Section VIII.
15.	Is the complete and unedited customer list a requirement for this RFP?	Yes. See RFP Section VI, B.
16.	Please elaborate on what the technology audit should entail. The Scope of Services enumerates the areas and systems that should be audited, but it is vague on the type of audit required. We understand the NHJB would like best practices for Active Directory configuration and change management control but would like clarity on the other services within scope.	Systems in scope should be reviewed for known vulnerabilities, and configurations should be compared to STIG. Policies, Standards, and Procedures should be audited following either ISO 27001:2013 and/or NIST CSF. Findings should include a risk assessment, a simple list of known vulnerabilities is not sufficient.
17.	Should the audits be treated like cybersecurity risk assessments?	Yes

18.	On Page 4 in the first paragraph of the introduction, the RFP includes a requirement to provide training to the IT personnel to fill knowledge gaps. Can you expand on the expectations for this training.	Hands-on and by example. If remediating a finding, explain to the SME why it is a finding, and what is being done to remediate and the expected outcome of the remediation.
19.	Can the NHJB share if budget has already been allocated for this effort and, if so, what is the allocated budget?	Yes, there is a budget for this project. The budget estimate will not be shared publicly.
20.	Page 5 in the background section of the RFP describes the general organizational structure of the Judicial branch in New Hampshire. Does the NHJB's central IT cover all subdivisions of the branch, or are there any subdivisions responsible for their own IT that would still be in scope for this assessment?	Yes, the NHJB IT Department is responsible for all IT systems and services across the branch.
21.	Page 6 section a.2 (Resource) item ii of the RFP requires the vendor estimate the number of NHJB resources required to conduct the audit/assessment. Approximately how many people does the NHJB anticipate the assessor needing to interview to gain a better understanding of its current cybersecurity posture (vulnerabilities, threats, risks)?	The number of NHJB employees needing to be interviewed for the assessor to gain a better understanding of the overall security posture will be up to the assessor and their determination after initial discovery conversations. Estimate a minimum of 6 for IT and a minimum of 8 for business/court processes. However, depending on the domain being audited, participants may be higher or lower.
22.	On page 6, section a.3 (Scope) item iii the RFP describes the selection of one application/service from the service catalog. How many services and/or applications are in the catalog? Are all services listed within the catalog, or are there undocumented services that should be considered?	The current catalog of selected services to be audited contains 19 services/applications. This however is not an exhaustive list of items in the catalog. Not all are expected to be audited, as well as there may be services/applications not currently in the catalog.
23.	Will the written report combine findings and recommendations within a single report or will additional working sessions with NHJB be expected beyond the report to build a strategic direction based on findings?	The report should contain recommendations associated to findings based on risk assessment. Additional meetings and working sessions can be held, but will need to be defined in the proposal if that is the vendor's preferred methodology.
24.	The "Overview – Scope of Services" paragraph on pg 5 states that the vendor should follow the NIST Security Framework. Section B under this	Both the NIST CSF and ISO 27001 can be used for audit purposes. The NHJB has an Information Security Plan built on the NIST CSF, so audits done using ISO 27001 must link

	paragraph states either NIST or ISO. Later on pg 6 under 2.a., it states that the vendors will select two domains from ISO. Please confirm that either the NIST CSF or ISO 27001:27002 can be used and whether or not one is preferred over the other.	to NIST CSF functional domains. NHJB does not have a preference on the vendors chosen audit modality, as long as it can be linked to NIST CSF functional sections and sub-sections.
25.	Are automated tools allowed to be used to assist with the assessment services?	Yes
26.	Since there will be numerous devices in the NHJB infrastructure which comply or aspire to comply with Windows Server STIG, is the expectation to evaluate the established configuration policy with the assumption that NHJB has good configuration management processes and applies those policies across the board to all devices? OR Is the vendor expected to evaluate STIG compliance for every device? If yes, what's an approximate number of computing devices and CISCO devices in use?	NHJB expects a review of both the configuration policy and change management processes, followed by a selection of devices to be reviewed for compliance. NHJB does not expect every device to be reviewed in an individual audit. NHJB does expect a subset of each device type to be reviewed for compliance. NHJB does expect that each subsequent audit will review a subset of previously audited devices for compliance in addition to new devices not previously audited.
27.	What is the size of NHJB's Active Directory environment in terms of users and organizational units?	1300 accounts, this is exhaustive of service and user accounts. 685 OUs
28.	In the Audit Preparation Planning section, the RFP asks the vendor to select 2 domains for an audit. In the Information Security Audit section, the RFP states that vendor will be provided with 2 domains to audit where NHJB performed poorly. Additionally, this section calls for the vendor to perform audit on 2 new sections. Can you confirm that the vendor will be required to perform an audit on 4 sections in total as a part of the ask in this RFP?	Yes, two previous and two new domains per audit, for a total of 4 domains per audit.
29.	In the Audit Preparation Planning section, the RFP asks the vendor to select 2 domains to audit instead of allocating the domains to the vendor. Is this interpretation correct? OR Will the vendor be assigned domains to audit?	For the initial audit, NHJB will select two previously audited domains, and the vendor will also choose two additional domains to audit. Subsequent audits, the vendor will choose a total of 4 domains to audit, two of which will have been audited previously.

30.	In the Audit Preparation Planning section, the RFP asks the vendor to specify at least 2 policies to review for regulatory compliance and process alignment instead of allocating the policies to the vendor. Is this interpretation correct? Or will the vendor be assigned Policies to review?	Correct, the vendor will select the policies to audit for regulatory compliance. NHJB and the vendor may choose to collaborate on which policies are to be audited if that process is more agreeable to the vendor and NHJB.
31.	How will the decision be made to select a production application or service for review during the Technology Audit? Can NHJB provide more information on the organizational risk criteria?	Applications will be selected based on public exposure of the application as well as the nature/sensitivity of the data the application has access to.
32.	Is NHJB currently ISO 27001:2013 certified, if not, is NHJB planning to obtain ISO27001:2013 certification?	No, the NHJB is not ISO 27001:2013 certified. No, the NHJB does not have any plans to become ISO 27001:2013 certified. The NHJB does expect audits to follow industry established standards and best practices outlined by either the ISO 27001:2013 or NIST CSF. Independent/Proprietary and/or non-industry recognized security auditing practices and methodologies will not be accepted.
33.	The RFP asks for the vendor to perform an audit but does not explicitly ask the vendor to provide a compliance certification. Is NHJB planning to use the outcomes of the Audit (assessment) to attest compliance OR is NHJB planning to use the outcomes of the audit to prepare for a more formal ISO27001:2013 certification later? Is it fair to assume that the vendor's audit report does not necessarily need to certify or attest NHJB with any compliance for the decided sections?	The NHJB is not seeking ISO certification, and does not need the vendor to formally attest/certify compliance. A simple statement in the audit documentation pointing out compliance/non-compliance suffices.
34.	What specific tasks are required to be on-site?	Any auditing process that requires physical access or physical review of systems/services. Those items can be discussed during discovery. Executive briefings with senior leadership are preferred in-person.
35.	Does NHJB want the selected vendor to perform the two (2) audits against the Annex A domains of ISO 27001:2013? (page 6 , section 2A Audit preparation planning)	Only if recommended based on risk assessments. Audits should focus on sections 4.1 – 10.2. Items in Annex A can be reviewed if risk assessments find them relevant.

36.	Can NHJB confirm that the two (2) audits will include 6 sections / domains each? (page 6, section B1 ISO 27001 Audit)	4 domains each audit. Two domains from a previous audit, and two new domains.
37.	How many staff in information/cyber security?	1
38.	Is IT and Security managed centrally?	Yes
39.	Can you provide the /types of devices for the device configuration review? (page 5, section A Overview scope of services)	Windows Server 2016, 2019, 2022 Cisco Switches, Routers, WAPs, WAP Controllers, and FirePower firewalls. ASR1002, C9300, C9606R, C9800, ISR4431, WS-C2960XR, AIR-AP4800
40.	Since the work is only for 100 hours can we propose a single auditor, who can perform all the duties or we need to propose two separate IT auditors? (Section IV. PROPOSED SCOPE OF WORK!! Sub section A. Overview - Scope of Services Page# 5).	100 hours is for remediation work, not for the actual audits. Performing the audit and associated findings is not part of the 100 hours of remediation work. If the vendor has an appropriate individual with all relevant experience and industry certifications, yes a single auditor can perform the work. Section IV. B.
41.	If the proposed candidate(s) are not available at the time of actual work request, can we provide the replacement candidate(s)? (Section IV. PROPOSED SCOPE OF WORK!! Sub section c. Remediation Hours Page# 7)	Yes, as long as all requirements are met and the NHJB agrees to the replacement.
42.	If the proposed 100 hours consulting work needs to be done together or In parts, meaning the 100 hours of work will be executed weekly/monthly/quarterly or otherwise. (Section IV. PROPOSED SCOPE OF WORK!! Sub section c. Remediation Hours Page# 7).	Work can be scheduled in a manner that works for both the vendor and the NHJB. The 100 hours is for the 12 months. Additional hours would need written approval prior to work performed. All work must be agreed upon beforehand.
43.	Is there an incumbent who is currently providing these services?	Yes.
44.	Is the incumbent eligible to bid on this contract?	Yes.

Vendor requested changes to the NHJB standard contract terms and conditions:

	RFP Contract Reference	**Requested Changes**	**NHJB Responses**
1.	Would the NHJB consider the following changes to Appendix A, Section 10?	**10. Insurance.** Contractor shall, at its sole expense, obtain and maintain in force, and shall require any sub-contractor or assignee to obtain and maintain in force, ~~comprehensive~~ commercial general liability coverage against all claims of bodily injury, death or property damage, in amounts of not less than $1,000,000 per occurrence and $2,000,000 in aggregate.	The change is acceptable to the NHJB.
2.	Would the NHJB consider the following changes to Appendix A, Section 15?	**15. Indemnification.** The Contractor shall defend, indemnify, and hold harmless the NHJB and/or the State of New Hampshire, its officers and employees, from and against any claims, liabilities and costs for any (a) personal injury or property damages, or (b) patent or copyright infringement, ~~or other claims or losses~~ asserted against the NHJB and/or the State of New Hampshire, its agencies, officers and employees~~, and any and all claims, liabilities or penalties asserted against the NHJB and/or the State of New Hampshire, its agencies, officers and employees~~, by or on behalf of any person, on account of, based or resulting from, arising out of (or which may be claimed to arise out of), in whole or in part, the negligence or willful misconduct of the Contractor under ~~acts or omissions of~~ the Contract~~Agreement~~. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the NHJB and/or the State of New Hampshire. This paragraph shall survive the termination of the Contract.	The NHJB is open to negotiation.
3.	Would the NHJB consider the following changes to	b. Provide fees to cover costs to NHJB ~~Assume responsibility~~ for informing all individuals in accordance with applicable law; and	The request is rejected.

	Appendix A, Section 19(b)?		
4.	Would the NHJB consider the following changes to Appendix A, Section 20?	**20. Event of Default/Remedies.** **20.1 Default.** Any one of the following acts or omissions by the Contractor shall constitute an event of default hereunder: a. Failure to perform the services as required hereunder ~~to the reasonable satisfaction of the NHJB~~ or on any agreed to schedule; or b. Failure to perform any other covenant, term, or condition of the Contract. **20.2 Remedy.** In the event of a default, the NHJB may take any or all of the following actions: a. Provide the Contractor with a written notice specifying the event of default and requiring it to be remedied within a reasonable period of time ~~determined by the NHJB to be sufficiently adequate~~ under the circumstances; and if the event of default is not remedied within the prescribed period, terminate the Contract effective two (2) days after the Contractor has failed to timely remedy the alleged default within the reasonable period provided; and b. Treat the Contract as breached and pursue any of its remedies at law, or in equity, or both unless Contractor cures the breach as permitted in paragraph a.	The NHJB is open to negotiation.