REQUEST FOR PROPOSALS

PROPOSAL DUE DATE : 4:00 p.m. MDST October 19, 2021

DESCRIPTION : The Navajo Nation Department of Information Technology under the Division of General Services is requesting proposals for Penetration Testing & Vulnerability Assessment located in Window Rock, AZ.

Advertisements: http://www.nnooc.org/RFPs-Advertisements.html

RE-BID NUMBER :

CONTACT PERSON :

Angelo James
Information Security Officer
Phone Number: (928) 871-6520
Email: ajames@navajo-nsn.gov
Fax Number: (928) 871-7737

DELIVER TO :

The Navajo Nation
Department of Information Technology
P.O. Box 5970
Tribal Hill Drive, Building No. W008-076
Window Rock, AZ 86515
Attn: Angelo James
Bid No. 21-09-2582LE

Please Submit Four (4) sets of your Proposal

REQUEST FOR PROPOSAL
Penetration Testing &Vulnerability Assessment
BID NO. 21-09-2582LE

SECTION I

A. **ISSUING OFFICE:** This Request for Proposal (RFP) is issued by the Navajo Nation Department of Information Technology (NNDIT), Division of General Services, Navajo Nation, P.O. Box 5970, Window Rock, Arizona. The contact person for this RFP is Mr. Angelo James, Information Security Officer, NNDIT.

B. **PURPOSE:** This RFP provides prospective respondents with sufficient information to enable them to prepare and submit a proposal for consideration.

C. **SCOPE:** This RFP contains the instructions governing the proposal to be submitted and the material to be included therein; mandatory requirements which must be met to be eligible for consideration; and other requirements to be met by each proposal.

D. **PROCUREMENT OF RFP:**

This procurement shall be conducted in accordance with all applicable Navajo Nation laws and regulations including the Navajo Business Opportunity Act http://www.navajobusiness.com/doingBusiness/Registration/CertReg.htm. All applicable rules, regulations, and laws shall also be followed. Prospective Vendors shall familiarize themselves with Navajo Nation regulations prior to submitting responses to this RFP and may request a copy of Navajo Nation procurement regulations from the NNDIT Information Security Officer at any time up to the Deadline for Proposals.

E. **SCHEDULE OF ACTIVITIES:** **DEADLINE:**

1.	Public Advertisement	October 04, 2021
2.	Inquiry deadline	October 14, 2021
3.	Due date for proposal	October 19, 2021
4.	Opening of proposals and evaluation by	October 22, 2021
5.	Review Team or Program Manager	October 26, 2021
6.	Award date for contract	October 27, 2021

F. **INQUIRIES:** Prospective respondents shall make written questions concerning this RFP to obtain clarification of requirements through e-mail to Angelo James, Information Security Officer, NNDIT at ajames@navajo-nsn.gov No inquiries will be accepted after the inquiry deadline listed in section E.

G. **ADDENDUM OF SUPPLEMENT TO THIS REQUEST FOR PROPOSALS:** In the event that it becomes necessary to revise any part of this RFP, an addendum will be issued.

H. **PROPOSAL SUBMISSION:** Proposal must be received on or before 4:00 p.m., October 19, 2021 (MDST). Respondents who are mailing their proposals should allow sufficient time for mail delivery to ensure receipt by the time specified. If mailed, it is recommended that proposals be sent by certified mail to the address indicated on the cover sheet of the RFP. No electronic proposals. **Late proposal will not be accepted.**

REQUEST FOR PROPOSAL
Penetration Testing &Vulnerability Assessment
BID NO. 21-09-2582LE

I. **FOUR SETS OF PROPOSAL AND TWO COPIES OF COST PROPOSAL ARE REQUIRED:** Each Respondent must submit in a sealed envelope one (1) original Proposal, three (3) additional Proposal copies, and two (2) copies of the Cost Proposal in a SEPARATE sealed envelope marked "cost proposal contained within" respondent's sealed proposal. The outside of the main 'Certified Mail' envelope should be clearly marked with the project name**- "Penetration Testing** &**Vulnerability Assessment" Proposal BID NO. 21-09-2582LE**–and the name and address of the firm submitting the proposal. **Proposal not clearly mark will not be accepted**

The NNDIT will not be liable to any Respondent for any unforeseen circumstances, delivery, or postal delays. Postmarking on or before, Tuesday, October 19th, 2021, by 4:00 p.m. (MST) will not substitute for receipt of the Proposal. Each Respondent is responsible for submission of their Proposal. Additional time will not be granted to a single Respondent.
A proposal will be disqualified if:
1. The cost proposal is not contained within a separate sealed envelope.
2. The cost proposal is submitted as part of the digital copy. Provide cost proposal in hard copy only.

J. **REJECTION OF PROPOSALS:** NNDIT reserves the right to reject any and all proposals. This RFP may be canceled at any time and all proposals may be rejected in whole or in part when the NNDIT Department Director determines it is in the best interest of the Navajo Nation.

K. **PROPRIETARY INFORMATION:** Any restriction on the use of data contained within any proposals must be clearly stated in the proposal itself. Proprietary information submitted in response to this RFP will be handled in accordance with applicable purchasing procedures. Each and every page of the proprietary material **must be** labeled or identified with the word **"proprietary".**

L. **RESPONSE MATERIAL OWNERSHIP:** All material submitted regarding this RFP shall become the property of The Navajo Nation and will not be returned to the respondent. Responses received will be retained by NNDIT and may be reviewed by any person after final selection has been made, subject to paragraph I above. NNDIT has the right to use any or all system ideas presented in reply to this RFP, subject to limitations in paragraph I above. Disqualification or non-selection of a respondent or proposal does not eliminate this right.

M. **INCURRING COSTS:** NNDIT is not liable for any cost by the respondents prior to issuance of a contract.

N. **ACCEPTANCE TIME:** NNDIT intends to make a vendor selection within four (4) working days after the closing date for receipt of proposals.

O. **SUFFICIENT APPROPRIATION:**
A contract awarded as a result of this RFP is contingent upon the availability of funds. A contract may be terminated or reduced in scope if sufficient funds do not exist. Sending a written notice to the Vendor shall effect such termination or reduction in scope. The NNDIT Department Director's decision to terminate or reduce the scope due to insufficient appropriations shall be accepted as final by the Vendor.

P. EVALUATION PROCEDURES AND CRITERIA:

1. An evaluation team will judge the proposals received in accordance with the general criteria used herein. Respondents should be prepared to provide any additional information the team feels necessary for the fair evaluation of proposals.

2. Failure of a respondent to provide any information requested in the RFP may result in disqualification of the proposal. All proposals must be endorsed with the signature of a responsible official having the authority to bind the respondent to the execution of a contract.

3. The sole objective of the review team will be to select the respondent who is most responsive to the needs of NNDIT. The specifications in this RFP represent the minimum performance necessary for a response. On the basis of the evaluation criteria established in this RFP, the review team will select and recommend the respondent who best meets this objective. If there is only one responsive bid, the NNDIT Department Director may elect to evaluate RFP solely.

4. Each bid must be accompanied by a letter of transmittal. The letter of transmittal must:

    1. Provide Statements of Qualifications
    2. Identify the name of the person responding to the RFP.
    3. Identify the name, title, and telephone numbers of person authorized to negotiate on behalf of the organization;
    4. Identify the names, and telephone numbers of person to be contacted for clarification;
    5. Navajo Preference, Certificate of Eligibility issued by the Navajo Business Regulatory Department
    6. Required insurance documents, i.e. Certificate of Liability Insurance
    7. Completed and signed W-9 Form
    8. Completed and Signed Navajo Nation Certification Regarding Debarment and Suspension
    9. No Subcontractors.
    10. Explicitly indicate acceptance of the conditions governing this procurement;
    11. Be signed by the person responding to the RFP; and
    12. Acknowledge receipt of any and all amendments to the RFP.

REQUEST FOR PROPOSAL
Penetration Testing &Vulnerability Assessment
BID NO. 21-09-2582LE

5. Evaluation Criteria: The following criteria will be used by an ad-hoc committee in the selection process for contract award. Vendors and proposals will be evaluated to determine the best opportunity for NNDIT.

Initial Point Criteria:

Evaluation Criteria	
http://www.navajobusiness.com/doingBusiness/Registration/NBOA/Cert_process.htm Priority 1 or 2 vendor a. Priority One vendor (10 pts.) b. Priority Two vendor (5 pts.) c. Non-Priority vendor (0 pts.)	10
Bid Organization a. Typed written on 8-1/2" X 11" paper b. Binding and indexing c. One original bid and 3 copies	10
Letter of Transmittal a. Provide Statements of Qualifications. b. Identifying individual(s) as specified above. c. List of similar services provided to other business customers on Navajo Nation in proportion to requested Scope of work	15
Proposed Workplan a. Provide a detailed and comprehensive description of how the Respondent intends to complete the SOW in this RFP. b. This discussion shall include, but not be limited to items requested in SOW including an overall construction schedule.	30
Cost Proposal a. Include in a separate sealed envelope clearly marked "Cost Proposal Contained Within" b. The cost proposed must include the total estimated cost breakdown for the project; Travel, Lodging, Meal, Rental, Labor, Material, Mobilization, Permits task. c. 5-year Annual Pen Testing and Remediation Cost for FY22 – FY26. The cost proposed must include yearly scan cost breakdown and the cost to fix all security findings.	25
Attachments a. Activity timeline and diagram method. b. Provide warranty, if applicable. c. Provide a sample of the diagram and test reports.	10
Total Score	100

-

Q. **STANDARD CONTRACT:** The Navajo Nation reserves the right to incorporate standard contract provision into any contract negotiations as a result of a proposal submitted in response to the RFP.

R. **TAX:**
All appropriate taxes should be **included in the cost of services including the Navajo Sales Tax.** All work performed within the territorial jurisdiction of the Navajo Nation is

subject to the Navajo Sales Tax of 6% (24 N.N.C. Section 601 et. seq.).

S. **TERM:** The term of this contract will be for a period of 5 years from the date of award.

U. **SOVEREIGNTY:** The Navajo Nation will not relinquish any of its sovereignty rights.

V. **COMPLIANCE WITH LAWS AND REGULATIONS:**
The successful Vendor shall comply with all Federal, Tribal, State, and Local laws, regulations and Navajo Nation rules and policies pertaining to work under its charge, and shall, at its expense, procure any permits that may be required.

W. **INDEMNIFICATION:**
To the fullest extent permitted by law, or as otherwise defined in the Contract, the successful Vendor shall indemnify and hold harmless the Navajo Nation and its officials, employees and agents from and against all claims, liens or demands that result in losses, liabilities, defense costs and expenses (including but not limited to attorney's fees and costs of litigation) arising out of the term, conditions and performance under the contract. The Vendor further agrees to indemnify and hold harmless the Navajo Nation, its agents, or employees, against claims or liability arising from or based upon the violation of any federal, state, county, city, or other applicable laws, bylaws, ordinances, or regulations by the Vendor, its agents, associates, or employees.

The indemnification provided above shall obligate the Vendor to defend at its own expense or to provide for such defense, at the Navajo Nation's option, of any and all claims of liability and all suits and actions of every name and description that may be brought against the Navajo Nation which may result from the operations and activities under any Contract resulting from this RFP.

The award of this Contract to the Vendor shall obligate the Vendor to comply with the foregoing indemnity provision.

SECTION II

A. BACKGROUND

The Navajo Nation Department of Information Technology (NNDIT) within the Division of General Services is responsible for Data Center located in Window Rock, AZ. NNDIT administering, managing, and planning for the Information Technology and activities for the Navajo Nation governmental offices.

B. SCOPE OF WORK:

The scope of this Penetration Test & Vulnerability Assessment services contract for Navajo Nation Department of Information Technology includes the following:

The scope of work for the threat Risk Assessment and Vulnerability Analysis is for the sole purpose of identifying, classifying and mitigating any risk found during the assessment to effectively assess and evaluate the security measures and identify all risks to the security of information because of the architecture and the configuration of the infrastructure implemented.

This assessment requires a detailed list of vulnerabilities and recommended mitigations for the risks associated with each of them, including but not limited to the following:

- Firewalls
- Routers and Switches
- Remote Access (VPNs)
- Physical Security
- WAN/LAN/WIFI Infrastructure
- Wireless Security
- Endpoint security controls
- Desktop, Laptop, Tablet, and Smart Phone encryption and security implementation
- Antivirus, Spyware and Malicious code detection
- Safeguards and controls to deter APTs (Advanced Persistent Threats)
- Incident and Response Reporting
- IT Policies and Procedures
- Documentation

REQUIREMENTS/TASKS

The contractor shall provide the knowledge, skills, abilities, staff support, and other related resources necessary to conduct a Penetration Test:

- Risk and Vulnerability Assessment
- Security Architecture Review
- System Security Engineering

Risk and Vulnerability Assessment (RVA)

RVAs conduct assessments of threats and vulnerabilities; determine deviations from acceptable configurations, enterprise, or local policy; assess the level of risk; and develop and/or recommend

appropriate mitigation countermeasures in operational and non-operational situations. Tasks include, but are not limited to:

- Penetration Testing
- Network Mapping
- Vulnerability Scanning
- Phishing Assessment
- Wireless Assessment
- Public facing IT services
- Identify services that need 2 factor-authentication
- Web Application Assessment
- Operating System Security Assessment (OSSA)
- Database Assessment
- Each risk level will be assigned. Risk level values of Critical, High, Medium or low. Ease of fix levels: Easy, moderately difficult, and very difficult or no known fix etc.

Subtask 1 - Penetration Testing

The contractor shall provide both internal and external security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. Black box testing will be done before any other testing. Deliverables for Penetration Testing include, but are not limited to, a Rules of Engagement document containing the type and scope of testing, and client contact details; and a Penetration Test Report that includes an executive summary, a contextualized walkthrough of technical risks, potential impact of vulnerabilities found, and vulnerability remediation options.

Knowledge and skills required for Penetration Testing include, but are not limited to:

- Knowledge of system and application security threats and vulnerabilities
- Skill in the use of social engineering techniques
- Skill in using penetration testing tools
- Knowledge of general attack stages

Subtask 2 - Network Mapping

The contractor shall identify assets on an agreed upon IP address space or network range(s). Deliverables for Network Mapping include but are not limited to a network map of the organization’s system that includes a visual representation of the organization's physical devices and digital network.

Knowledge and skills required for Network Mapping include but are not limited to:

- Knowledge of network security architecture concepts including topology, protocols, components, and principles
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration Protocol (DHCP), domain name system, and directory services
- Ability to generate and implement capabilities to monitor the organization’s network in real-time

Subtask 3 - Vulnerability Scanning

The contractor shall comprehensively identify IT vulnerabilities associated with Navajo Nation systems that are potentially exploitable by attackers. Deliverables for vulnerability scanning include but are not limited to a Vulnerability Scanning Risk Assessment that includes an executive summary and risk assessment reports and/or dashboards.

Knowledge and skills required for Vulnerability Scanning include but are not limited to:

- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in using network analysis tools to identify vulnerabilities
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data

Subtask 4 - Phishing Assessment

The contractor shall complete activities to evaluate the level of awareness of the Navajo Nation workforce regarding digital form of social engineering that uses authentic looking, but falsified, emails requesting information from users or direct them to a fake website that requests information. Phishing assessments can be conducted as a one-time event or as part of a larger campaign to be conducted over several months. Deliverables for a Phishing Assessment include, but are not limited to, a Phishing Assessment Report that includes an executive summary and metrics that highlight potential weaknesses in an organization's email policy.

Knowledge and skills required for a Phishing Assessment include but are not limited to:

- Skill in the use of digital social engineering techniques

Subtask 5 - Wireless Assessment

The contractor shall include wireless access point detection, penetration testing, or both. A wireless assessment is performed while onsite at a customer’s facility. Deliverables for a Wireless Assessment include but are not limited to a Wireless Assessment Report that includes an executive summary, networking mapping, vulnerability analysis, and a wireless network configuration assessment on the wireless system.

Knowledge and skills required for a Wireless Assessment include but are not limited to:

- Knowledge of wireless security threats and vulnerabilities
- Skill in the use of social engineering techniques
- Knowledge of general attack stages

Subtask 6 - Web Application Assessment

The contractor shall provide a Web Application Assessment that includes scanning, testing, or both of outward facing web applications for defects in web service implementation that may lead to exploitable vulnerabilities. Deliverables for Web Application Assessment include but are not limited to a Web Application Assessment Report that indicates whether traditional network security tools and techniques are used to limit access to the web service to only those networks and systems that should have legitimate access.

Knowledge and skills required for a Web Application Assessment include but are not limited to:

- Knowledge of system and application security threats and vulnerabilities
- Skill in the use of social engineering techniques
- Knowledge of general attack stages

Subtask 7 - Operating System Security Assessment (OSSA)

The contractor shall assess the configuration of select host operating systems against standardized configuration baselines. Deliverables for OSSA include but are not limited to an OSSA Report that includes an executive summary and a vulnerability analysis.

Knowledge and skills required for OSSA include but are not limited to:

- Knowledge of organizational baselines and configuration management systems
- Knowledge of security content automation protocols (SCAP) and operating system hardening guidelines
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data

Subtask 8 - Database Assessment

The contractor shall assess the configuration of selected databases against configuration baselines to identify potential misconfigurations and/or database vulnerabilities. Deliverables for Database Assessment include but are not limited to a Database Assessment Report that includes an executive summary, privacy assessment, and vulnerability assessment.

Knowledge and skills required for a Database Assessment include but are not limited to:

- Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
- Knowledge of database security threats and vulnerabilities
- Knowledge of relational database management systems (RDBMS)

Security Architecture Review (SAR)

SAR evaluates a subset of the Navajo Nation's HVA security posture to determine whether the Navajo Nation has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA's individual security components integrate and operate, including how data is protected during operations. Architecture strengths and findings are documented in a SAR Report.

Knowledge and skills required for a SAR include but are not limited to:

- Ability to perform architecture design reviews
- Ability to perform system configuration and log reviews
- Ability to perform network traffic analyses

System Security Engineering (SSE)

SSE identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle.

The contractor shall provide system engineering and architectural design support services. All strategic engineering activities will be defined and scheduled by Navajo Nation Department of IT. These directed services include:

- Studies and analysis of proposed operations modifications
- Identification and documentation of alternative operations solutions
- End-to-end architecture tradeoff assessment
- Development of strategic and tactical plans
- Implementation plans and strategies
- Standards development
- Evaluation of new program requirements
- Investigation and development of new technologies for possible operations modifications

Recommendation Identify, analyze, and confirm vulnerabilities solutions

The vendor will supply solutions and remediation recommendations on the vulnerabilities identified. The solutions and recommendations will utilize the best practices from security implementation and configuration. Provide all solutions in a phased approached and considering Industry Compliance approach will include HIPAA Compliance, ISO security standard, etc.

Fixed Fee to include all Travel and Out-of-Pocket Expenses

Bidder must include all travel, living, meals, materials, incidentals, out-of-pocket, and other expenses as part of its price proposal. Bidder is to provide documentation substantiating the amount of the fixed fee attributable to travel, out-of-pocket and other expenses, including the estimated number of flights, hotel stay nights or other accommodations used by Bidder to develop the fixed fee.

Phase approached cost for scope of work

5-year Annual Pen Testing and Remediation Cost for FY22 – FY26. The cost proposed must include yearly scan cost breakdown and the cost to fix all security findings.

Respondents will also:

Provide a detailed and comprehensive description of how the Respondent intends to complete the SOW in this RFP.

Provide the cost proposed. Must include the total estimated cost breakdown for the project; Travel, Lodging, Meal, Rental, Labor, Material, Mobilization, Permits task.

Provide a Project Plan Schedule of tasks with periodic checkpoints, status reports, progress, issues, next steps and priorities where deliverable reports are appropriate.

Provide list of credentials. No subcontractors. All personnel will be certified.

REFERENCES

The contractor shall be familiar with Federal policies, program standards, and guidelines such as, but not limited to, those listed below, or later versions as amended:

REFERENCE	DESCRIPTION / TITLE
FISMA	*Federal Information System Modernization Act (FISMA) (2014)*
FIPS 199	*Federal Information Processing Standards (FIPS) Publication 199 - Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*
NIST SP 800-30 Rev 1	*National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments*
NIST SP 800-35	*Guide to Information Technology Security Services*
NIST SP 800-37 Rev 2	*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
NIST SP 800-39	*Managing Information Security Risk: Organization, Mission, and Information System View*
NIST SP 800-44 Version 2	*Guidelines on Securing Public Web Servers*
NIST SP 800-53 Rev 4	*Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-53A Rev 4	*Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
NIST SP 800-61 Rev 2	*Computer Security Incident Handling Guide*
NIST SP 800-83 Rev 1	*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
NIST SP 800-86	*Guide to Integrating Forensic Techniques into Incident Response*
NIST SP 800-101 Rev 1	*Guidelines on Mobile Device Forensics*
NIST SP 800-115	*Technical Guide to Information Security Testing and Assessment*
NIST SP 800-128	*Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-137	*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
NIST SP 800-150	*Guide to Cyber Threat Information Sharing*
NIST SP 800-153	*Guidelines for Securing Wireless Local Area Networks (WLANs)*
NIST SP 800-160 Vol 1	*Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
NIST SP 800-171 Rev 1	*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
NIST SP 800-171A	*Assessing Security Requirements for Controlled Unclassified Information*
NIST SP 800-181	*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
P.L. 93-579	*Public Law 93-579 Privacy Act, December 1974 (Privacy Act)*
40 U.S.C. 11331	*Responsibilities for Federal Information Systems Standards*
OMB M-19-03	*Office of Management and Budget (OMB) Memorandum 19-03,*

REFERENCE	DESCRIPTION / TITLE
	Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
OMB A-130	*OMB Circular A-130, Managing Information as a Strategic Resource*
BOD 18-02	*Department of Homeland Security's Binding Operational Directive 18-02, Securing High Value Assets*