2/12/2025

ADDENDUM #2 –QUESTIONS/ANSWERS

FOR RFP –Third-Party Risk Management Solution

1. I see in the proposal, that you're requesting a quote for "up to fifty third-party entities." Approximately how many of these entities are located outside of the US or Canada? **None**

2. D&B offers several analytics to assist with your organization risk assessments that are considered an "add-on" to our standard offering. After reading the RFP, I'm not able to determine which (if any) of these are of interest to the Cherokee Nation. Can you please offer some insight?
   - **ESG Intelligency:** Designed to help you incorporate environmental, social and governance evaluation components into your risk management processes to help manage risk, increase supply chain resiliency, and drive entity performance. **Not needed**
   - **Cyber Risk:** Helping your team to evaluate and understand potential cyber risks the supplier could impose. Not needed
   - **Enhanced Screening:** Company principals and beneficial owners are screened for PEP's, watchlists, sanctions, SOE, and adverse media. **Not needed**

3. What is the target go-live date for the solution? Is this the September 30, 2025, date listed? Or would the September 30th

date include completion of the 50 assessments within the solution? **Go live should be as soon as the software solution has been activated. Our team will add our vendors in the continuous monitoring and management solution as well as develop questionnaires relevant to our environment.**

4. Are you able to provide a list of all potential integrations to existing systems? **The bid response should list the integrations available or provide a website link to existing solution integrations.**

5. Is Single Sign-On (SSO) required for internal access? **No**

6. Please describe your current state TPRM program.
   a. What type of vendors are included in the TPRM portfolio? Are vendors categorized? If so, in what manner? **Information technology vendors.**

   b. What is the current process for performing risk assessments? If questionnaires are sent, how many questions and artifacts are requested? **A questionnaire of approximately 120 questions is sent to vendors and supporting**

documentation is requested as evidence of compliance with applicable.

c. Is there an existing inherent risk methodology that can be leveraged or is that something Crowe will help develop as part of the proposed services? **Cybersecurity risks are reviewed leveraging NIST frameworks.**

d. Is there an existing residual risk methodology that can be leveraged or is that something Crowe will help develop as part of the proposed services? **Residual risks are constantly evolving due to the nature of the changing cyber environment.**

e. Is there an existing findings management process to address action plans stemming from risk assessments? **Action plans should be standardized according to the identified risks found by the continual monitoring and vulnerability assessments of the TPRM solution with automatic notifications sent to the vendor which would be configured in the solution.**

7. Will assessment findings be sent externally, to the vendor, or assigned to the business owner and managed internally? **Sent to the vendor.**

8. Is there a need for the Crowe to perform the 50 risk assessments on behalf of CNIT, inclusive of managing action plans through remediation? **The TPRM solution should be capable of automation this after configuration of the solution.**

9. Does each in-scope risk domain require continuous monitoring capabilities? **Yes**

10. Does CNIT have defined KRIs and KPIs required to be included within the reporting an analytics? **The solution should be score based on US (NIST) industry standards.**

11. Are there any supplementary materials or specific compliance requirements we should be aware of? **NIST Special Publication 800 for cybersecurity**

12. **Term of Proposed Contract** –Is this negotiable? Our standard terms is a minimum of 12 months. **12 months is standard and if additional years are negotiated, there must be a cancellation clause at the end of each year.**

13. **Indemnification** –Is this negotiable? **No**

14. **FedRAMP Compliance –**Our solution enables clients to use FedRAMP as a framework. Does Cherokee Nation require its vendors to be FedRAMP-certified? **Preferred but not required**

15. Is Wissda Inc., registered in New Jersey, eligible to participate in this RFP? **As long as terms are agreed upon.**

16. As Wissda is not an Indian Organization nor TERO certified, can we still submit a proposal? **In the proposal it states proposals will be accepted from Indian and Non-Indian bidders. Yes**

17. Wissda specializes in TPRM consulting and will be providing the solution using an industry-leading platform as its certified implementation and reselling partner. Would this arrangement be considered subcontracting? **Yes**

18. Should the insurance coverage certificate be included with the RFP response, or can it be submitted upon vendor selection? **Please include**

19. A comprehensive risk management program is comprised of the following five elements: People, technology, data, regulatory, and third-party risk. Is this RFP for Third-Party Risk Management Solution part of a larger risk program? **The TPRM solution is for software and cloud environments.**

20. Is the effort to implement third-party risk solution driven by a regulatory requirement, i.e. is the Cherokee Nation required to have such solution implemented to pass compliance? If yes, could you please share the regulatory requirement with us? **No**

21. Does Cherokee Nation leverage a security framework (e.g., NIST Cybersecurity Framework) to be able to map third-party risk? **Yes**

22. Does Cherokee Nation expect to conduct the up to 50 third-party risk evaluations via a manual (questionnaire-based) process or via a software-based tool? **Automated process cloud based solution**

23. Does the Cherokee Nation currently use any technologies to fulfill the key requirements listed in the RFP scope? If so, could

you please provide the list of the existing technologies (e.g., ServiceNow)? **The bid response should list integration capabilities.**

24. Does The Cherokee Nation have a risk repository in place today? **Yes however it is manual.**

25. Does the Cherokee Nation anticipate the vendor providing ongoing managed services for the solution after successful implementation, configuration, and operationalization? **Only for the TPRM solution software.**

26. Is the vendor expected to conduct an initial risk assessment for up to 50 third-party entities as a baseline for ongoing monitoring? **No the risk assessment can be performed after configuration of the solution.**

27. Regarding the scope of services under bullet 2: Continuous monitoring (page 12), the RFP mentions “integration with relevant data sources to provide real-time insights”. Could you confirm that the relevant data sources include both internal and

external sources (e.g., BitSight, BlackKite, Security Scorecard). **External sources only meaning any public websites/presence.**

28. Regarding the Scope of Services under bullet 8: Vendor support and training (page 13), ongoing technical support, training, and documentation is mentioned. Could you provide additional detail on what Cherokee Nation is expecting as it relates to ongoing support of the solution? **The solution should have either online help or technical assistance for the TPRM software and ongoing support/training when new functionality is introduced.**