NORTH CAROLINA
DEPARTMENT OF REVENUE

Solicitation Addendum

Solicitation Number: 45-PR11914284

Solicitation Description: Managed Security Services

Solicitation Opening Date and Time: February 15, 2021 @ 2:00 PM EST

Addendum Number: 1

Addendum Date: February 1, 2021

Purchasing Agent: Nicole A. Hunter, Associate Director, Procurement and Contracts
DORProcurement@ncdor.gov, 919.814.1037

---

1. Return one properly executed copy of this addendum with bid response or prior to the Bid Opening Date/Time listed above.
2. The bid opening date has been extended. All bid responses are now due no later than 2:00 PM EST on Monday, February 15, 2021.
3. The solicitation is hereby **modified** as follows:

   M1. *IFB Section 3.7 Cloud Service Providers (CSPs). Reserved.*

   M2. *IFB Section 4.0 Furnish and Deliver*

4.0 FURNISH AND DELIVER

**Where applicable, Vendor must complete Quantity (QTY) and Unit of Measure (UOM) along with Unit Cost and Extended Cost for each line item.*

ITEM #	QTY*	UOM*	DESCRIPTION	UNIT COST	EXTENDED COST
1	12	Month	Year 1-Managed Security Operations Services		
2	1	Job	Professional Services for Implementation		
3			Hardware (including Year 1 Maintenance) This line must be itemized to address all required or recommended hardware for vendor's solution.		
4			Software (including Year 1 Maintenance)		

			This line item must be itemized to address all Vendor-owned and third party software required or recommended for Vendor's solution.		
5			Other Costs: This line item must be itemized and defined in detail and may not be accepted by NCDOR.		

Total Offer Cost _____

4.1 <u>OPTIONAL COSTS</u>—May or may not be purchased by the State

YEAR 2 OPTIONAL COSTS

ITEM #	QTY*	UOM*	DESCRIPTION	UNIT COST	EXTENDED COST
1	12	Month	Year 2 Managed Security Operations Services		
2	80	Hours	Ad Hoc Professional Services outside of managed security operations		
3			Year 2 Hardware Maintenance To include upgrades, patches, and support services of all required or recommended hardware for vendor's solution listed in Item #3 in the Furnish and Deliver Table.		
4			Year 2 Software Maintenance To include upgrades, patches, and support services of all required or recommended hardware for vendor's solution listed in Item #3 in the Furnish and Deliver Table.		
5			Other Costs: This line item must be itemized and defined in detail and may not be accepted by NCDOR.		

Total Optional Year 2 Costs _____

YEAR 3 OPTIONAL COSTS

ITEM #	QTY*	UOM*	DESCRIPTION	UNIT COST	EXTENDED COST
1	12	Month	Year 3 Managed Security Operations Services		
2	80	Hours	Ad hoc Professional Services outside of managed security operations		
3			Year 3 Hardware Maintenance To include upgrades, patches, and support services of all required or recommended hardware for vendor's solution listed in Item #3 in the Furnish and Deliver Table.		
4			Year 3 Software Maintenance To include upgrades, patches, and support services of all required or recommended hardware for vendor's solution listed in Item #3 in the Furnish and Deliver Table.		
5			Other Costs: This line item must be itemized and defined in detail and may not be accepted by NCDOR.		

Total Optional Year 3 Costs _____

4. Following are questions received about the solicitation and the State's answers to the questions.

Qstn	Citation	Vendor Question	State's Response
1	Page 11 Technical Specifications	What is the anticipated start date?	July 2021
2	Page 26 Scope of Work	Do you have an inventory of all the devices on the network or will a network inventory pull be required?	Yes
3	Page 26 Scope of Work	How many employees will be supported under the managed environment?	3000
4	Page 26 Scope of Work	Is there an estimated budget for this project?	Yes
5	3.7 Cloud Service Provider	Is FedRAMP required if my solution does not process, store, or transmit FTI, STI, or PII?	See M1 above.

Qstn	Citation	Vendor Question	State's Response
6	3.7 Cloud Service Provider	Please define the scope of a Cloud Service Provider.	See M1 above.
7	3.7 Cloud Service Provider	Can the NCDOR accept certification other than FedRAMP?	See M1 above.
8	2.14 Evaluation Criteria	Is there a US citizenship requirement for all SOC personnel?	Yes
9	2.14 Evaluation Criteria	Can we leverage global resources in tandem with US resources?	No
10	2.14 Evaluation Criteria	Is NCDOR looking for eyes on glass or eyes on alerts?	Eyes on glass
11	3 Scope of Work	What is the current average EPS throughput of the NCDOR instance of QRadar?	It varies on a day-to-day basis. Currently across both the console and event collector is approximately 17,000 EPS.
12	3 Scope of Work	Is Watson leveraged today?	No
13	3 Scope of Work	The RFP lists "SIEM instance and/or network detection devices". Please explain what the network detection devices are and how many devices there are in the environment. Should an incident response retainer be included as part of this bid?	 Palo Alto Firewalls-20 FireEye-2 F5-4 No
14	3 Scope of Work	What tool is NCDOR currently using for vulnerability management?	Nessus Security Center
15	3 Scope of Work	How many assets are scanned using the vulnerability management tool?	Approximately 3,000 resources are continuously monitored and scanned.
16	Section 3 Scope of Work	Please define remediation as it relates to vulnerability management.	Remediation is defined as Tier 1 and Tier 2 eyes on the glass. The vendor will not have access to NCDOR's security and network tools.
17	Section 3 Scope of Work	Will all devices be monitored through the SIEM?	No
18	Section 7.3 Incident Response Services	Should an incident response retainer be included as part of this bid?	See response to Question 13 above.

Qstn	Citation	Vendor Question	State's Response
19	Section 3.7	In reviewing the IFB proposal, we noticed in section 3.7 for CSPs there is a hard FedRAMP compliance at Moderate level or higher. I just wanted to confirm that the DOR will only be looking to work with organizations that are FedRAMP moderate certified and sponsored by a government agency?	See M1 above.
20	Section 3 SOW, Page 26 of 41	What is the make-up of the current security team that the vendor will share resources with? (i.e., skillsets such as Forensics Analyst, Engineers, etc.)	2 Architects, 2 Engineers, 3 Analysts.
21	Section 3 SOW, Page 26 of 41	How many team members make-up the SOC?	See response to Question 20 above.
22	Section 3 SOW, Page 26 of 41	How do you envision the shared services model? Specifically, how is the work divided, and what time of day? (i.e., weekends, days, nights, etc.)	Eyes on glass approach with 24/7 support, including weekends and holidays. See Attachment A—Scope of Work, Section 9.6. Vendor is expected to perform Tier 1 or 2 analysts for 24x7 monitoring.
23	Section 3 SOW, Page 26 of 41	What is the current number of events/incidents per day?	QRadar generates 10 offenses per day on average, sometimes less. These are typically not true positives, these items usually result in tuning.
24	Section 3 SOW, Page 26 of 41	Does NCDOR have a custom alert library inside of QRadar? If so, how many custom alerts have been built and implemented?	No. Alerting is turned off in QRadar due to the number of false positives.
25	Section 3 SOW, Page 26 of 41	How many log sources are currently ingested into QRadar?	642, possibly less once log source clean-up is done on our end.
26	Section 3 SOW, Page 26 of 41	What is the description of each source?	There's too many to list individually in this document. We have a variety of log source types to include: • Windows Servers (Domain Controllers, General Purpose) • Unix/Linux Servers • Email (Exchange, O365) • Security Devices (FireEye, McAfee ePO, ForcePoint) • Oracle Databases • Microsoft SQL Databases • Network Devices (Firewalls, F5, VPN, Switches)

Qstn	Citation	Vendor Question	State's Response
27	Section 7.3, Page 29 of 41	Does NCDOR have a current incident response policy in place?	Yes
28	Section 9, Page 33 of 41	Does NCDOR have a test environment for analysis?	Yes
29	N/A	Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - can you please provide incumbent contract number, dollar value and period of performance?	No
30	Attachment A	Specify the VLAN details how many is included in the Scope?	120 VLANS in all datacenters.
31	Attachment A	Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.)? Is there any External Interface need to Pentest? If yes then please specify details?	500 physical servers, 400 VMs, 100 network devices. Yes Domain ncdor.gov
32	Attachment A	Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking?	No. GRC ServiceNow module is in process.
33	Attachment A	Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name.	Yes QRadar
34	Attachment A	How many Active Directory Environment domain is included in Penetration testing?	2
35	Attachment A	We may use sampling for configuration review based on number and function of the system (Web server, file server, app server, database, firewall (int/ext), VPN, Load Balancer etc.).	Yes

Qstn	Citation	Vendor Question	State's Response
36	Attachment A	Do you want this as a red team exercise to test the SOC/NOC's response where they will get to see the results and update their Knowledge Base (KB) afterward or Blue team where we work with the SOC/NOC and share our attacks so they can update their KB during the testing?	Yes This should be a red team exercise.
37	Attachment A	How many physical locations are included in Pen testing?	2
38	Attachment A	Is "web application" security testing in scope? If yes, please provide number of applications, External facing (internet accessible) or Internal facing? How Many Web Application is in Scope for Pen testing? Specify if Any.	No
39	Attachment A	Do you manage your own data Center, or do you utilize any 3rd-party/ colocation facilities?	Both. We manage our Raleigh HQ datacenter and utilize a 3rd party colocation facility in RTP.
40	4.0 Furnish and Deliver / 4.1 Optional Costs (Page 12) Attachment A: Scope of Work (Page 26)	In order to determine pricing, some measure of volume of volume of work to be performed is needed. Could DOR please share all or any of the following data? ▪ An inventory of log sources, including QRadar sensors ▪ Ingestion volume ▪ Events per second ▪ Number of incidents per month by tier for the preceding 12 months ▪ Current number of use cases and runbooks	▪ 642 log sources, no QRadar sensors ▪ Peak EPS Currently – 17,000 ▪ QRadar generates ~ 30 Offenses per month, presumably false positives ▪ Use Cases – We have approximately 100 or more rules (use cases) enabled for threat detection. These our out-of-the box with a few custom. ▪ Runbooks – None. We have a QRadar monitoring guide, but no runbooks for individual incidents.
41	Attachment A: Scope of Work (Page 26)	Is supplier expected to use DOR's ticketing system?	No
42	Attachment A, 3-Scope of Work, RACI and 7.3, Incident Response Services (Page 29)	Is the supplier required to do the hands-on work of incident containment and remediation on State devices, or provide NCDOR personnel with expert support?	Supplier is required to provide NCDOR personnel with expert support. Remediation is defined as Tier 1 and Tier 2 eyes on the glass. The vendor will not have access to NCDOR security and network tools.
43	Page 27	Will NCDOR provide existing runbooks that are in use currently?	No

Qstn	Citation	Vendor Question	State's Response
44	Page 27	Will NCDIT provide existing runbooks that are in use currently for NCDOR?	No
45	Page 27	Does NCDOR currently use additional hardware or software to perform pre-filtering or manipulation of log data going into the SIEM?	No
46	Page 27	If NCDOR does perform log pre-filtering or manipulation, is the configuration, management, or monitoring of this also in scope for the services delivered under this SOW?	Yes, configuration, management, and monitoring of pre-filtering and manipulation of logs is in scope for services delivered under this SOW.
47	Page 27	Are respondents to this RFP expected to perform services related to the configuration, management, or monitoring of log sources outside of the required level needed to properly test and tune log generation?	Yes
48	Page 31	What system(s) are in place today to handle vulnerability management?	Nessus Security Center
49	Page 27	Do responders need to carry and provide OEM and/or acceptable 3rd party certifications for the systems supported under this SOW?	Yes
50	Page 30	What is the volume of offenses over the last 30 days?	70
51	Page 26	Does NCDOR currently have runbooks in place that will form the basis for any runbooks created by the selected vendor, or will the runbooks be created entirely by the vendor?	See response to Question 40 above. Runbooks will be created entirely by the vendor.
52		Is there an expected number of runbooks that are to be created, or are they expected to be created on an "as needed" basis?	Yes. Runbooks are also expected to be created as needed.
53	Page 27	Does NCDOR have an established use case management process that is used to standardize and verify the efficacy of use case tuning actions? If not, will the vendor be permitted to develop and implement such a process within the agency?	No Yes

Qstn	Citation	Vendor Question	State's Response
54	Page 9	Will consideration be given to vendors who provide a discount for an initial 2 year contract or is there any room to have the initial contract more than 1 year?	See Sections 3.11 Contract Term and 6.3 Prompt Payment Discounts. Vendors may note any pricing discounts in its response. However, the initial term is as noted in Section 3.11.
55	2.14. EVALUATION CRITERIA ix. Availability of additional incident response resources in the event of a breach (p. 8)	Incident response retainer services are available, pricing is not usually detailed until an opportunity is scoped. Is this service something that should be quoted with this IFB?	Yes
56	7.2 Malware Analysis and Forensics (p. 29)	NCDOR states that the Vendor "must be able to investigate and analyze malicious activity", what software are you currently using on your endpoints? Are you looking for the Vendor to provide management of this endpoint solution?	Palo Alto. McAfee, Encase. Only Palo Alto and McAfee log to QRadar. No
57	9.2 Subject to compliance with NCDOR security requirements, Vendor will connect to the NCDOR's SIEM environment remotely using TLS-encrypted web access configured by NCDOR for named resource accounts if applicable. (p.33)	Does NCDOR require the Vendor manage their existing SIEM in the existing infrastructure or can the events be exported into the Vendor's infrastructure?	Events can be exported into vendor's infrastructure.
58	7.3 Incident Response Services (p. 29)	In order to provide 24x7 Response capabilities, we offer a separate management option for some endpoint solutions and perimeter devices. Would NCDOR require this option as part of this IFB?	No
59	7.5 Extensive Vulnerability Management (p. 31)	We provide vulnerability management services that will fit your needs. For us to provide an accurate quote, we would need the following information: • # of external IPs to be scanned • # of internal IPs to be scanned • # of endpoints to be monitored	580 external IPs 10,000 internal IPs 3000 endpoints

Qstn	Citation	Vendor Question	State's Response
60	General Inquiries	In order to provide an accurate quote and correctly scope the project, it would be helpful to have some of the following information: • # of FWs (please provide vendor /model) • # of user endpoints • # of end users • # of servers • SaaS applications (i.e. O365, GSuite, etc.) • Cloud based infrastructure (i.e., AWS, GCP etc.)	20- Palo Alto/820, 3060. Cisco ASA 5516 3000 endpoints 3000 end users 500 servers 0365 Azure
61	NA	Is there a preferred contract vehicle?	The awarded vendor's response, this IFB, and any addendum thereto will become the contract vehicle.
62	RFP Section 2.14 Page 8	The technical evaluation criteria includes the ability to respond to detected attacks. Is there a managed endpoint detection and response component to this RFP? If so, does NCDOR have an EDR tool, or is managed EDR a requirement? If an EDR tool or MDR service is needed, please supply an endpoint device count to include workstations and servers as well as device OS. **Reference Text:** Ability to rapidly respond to detected attacks	No. Endpoint detection is handled in-house.
63	RFP Section 3.13.2 Page 11	Is the State requiring that we can only reference customers that are no longer our customers ("must have been completed in the past 3 years")? **Reference Text:** References. Vendor(s) must provide the names of three (3) private and/or public sector organizations for which Vendor has implemented and provided services similar in size and scope of the project outlined in ATTACHMENT A—Statement of Work. The relevant project referenced must have been completed in the past three (3) years.	No

Qstn	Citation	Vendor Question	State's Response
64	RFP Section 3.0 Page 26	Is management of QRadar required or simply the monitoring of the events and logs captured by QRadar? Please clarify our potential role and NCDOR's role regarding QRadar? **Reference Text:** Vendor will provide monitoring and remediation support for NCDOR's QRadar SIEM instance	No. Vendor shall monitor events and logs captured by QRadar. See the RACI model in Attachment A—Scope of Work, Section 3. See responses to Questions 16 and 42 regarding remediation and remediation support.
65	RFP Section 3.0 Page 26	What are the types and quantity of data sources that feed into the QRadar SIEM? Is NCDOR able to supply a daily data ingest volume or count of events per second? **Reference Text:** Vendor will provide monitoring and remediation support for NCDOR's QRadar SIEM instance	642 log sources. There's too many to list individually in this document. We have a variety of log source types to include: • Windows Servers (Domain Controllers, General Purpose) • Unix/Linux Servers • Email (Exchange, O365) • Security Devices (FireEye, McAfee ePO, ForcePoint) • Oracle Databases • Microsoft SQL Databases • Network Devices (Firewalls, F5, VPN, Switches) Yes
66	RFP Section 3.0 Page 26	Question: Is NCDOR able to provide a list of log sources per location (e.g., data center, cloud, site 1, site 2, etc.)? **Reference Text:** Vendor will provide monitoring and remediation support for NCDOR's QRadar SIEM instance	No
67	RFP Section 7.5 Page 31	Can you please supply the total number of IP's and/or total assets to be included in in the vulnerability management program? **Reference Text:** Extensive Vulnerability Management - The managed services must be able to provide continuous monitoring, mitigation, and remediation to protect NCDOR's network	580 external IPs 10,000 internal IPs Total assets are 5000

Qstn	Citation	Vendor Question	State's Response
68	Section 9.3, 9.6.2 Pg. 33	Does NCDOR have a licensed SOAR platform/solution ("Security Orchestration, Automation, and Response")? If yes, what is the Vendor's expected involvement with SOAR? Also, please provide details about the SOAR solution.	No
69	Section 7.2 Pg. 29 Section 9.6 Pg. 33	Does NCDOR have an EDR solution ("Endpoint Detection and Response") that needs to be integrated with the SIEM? If yes, is NCDOR requiring "Managed EDR" (also called "MDR") solution as a service?	Yes. Palo Alto, Encase, and McAfee No
70	9.6, 9.6.1 Pg. 33	Can you please clarify if you want the Responder/Vendor to provide all Tier 1 & Tier 2 resources?	Vendor should provide all Tier 1 and 2 resources.
71	Section 2.14 Pg. 8	Is NCDOR requiring US-based MSS personnel / resources? If yes, please elaborate on any specific detailed requirements, for e.g., data residency, data in transit, etc.	Yes. See Section 3.0 Specifications, subsection 3.2. See Attachment A—Scope of Work, subsection 8, IT Security Requirements. Vendor is expected to review the security policy manual referenced in Section 8.2 of the Scope of Work and Internal Revenue Publication 1075.
72	Section 2.14 Pg. 8	For example, can Vendor consider utilizing near-shore/off-shore resources for maintenance-and-support activities such as SIEM Administration and Engineering?	No
73	Section 7.5 Pg. 30	Does NCDOR already have a licensed vulnerability scanning / vulnerability management solution/tool(s)? If yes, please provide details about which tool, tool sizing, license terms, etc. If yes, please also clarify if Vendor is expected to manage the tool going forward.	Yes Nessus Security Center. No

Qstn	Citation	Vendor Question	State's Response
74	Section 7.5 Pg. 31	Is NCDOR requiring Vendor to develop and run a comprehensive / extensive Vulnerability Management Program? If yes, please provide technical details about your environment (i.e., total count of endpoints, servers, network devices, OS types, types of applications in your environment, etc.).	No 5000 endpoints 700 Servers 120 Network devices Linux/Windows/Palo, Proofpoint, FireEye, Cisco, Azure, McAfee,
75	Section 7.5 Pg. 31	What is the expected level of involvement for Vendor as it pertains to vulnerability remediation / mitigation activities, e.g. patch management, hands-on technical remediation implementation on NCDOR-owned systems, etc.?	See Attachment A—Scope of Work, Section 9. See response to Questions 16 and 42 regarding remediation and remediation support.
76	Section 7.6 Pg. 31	What Threat Intelligence feeds do you utilize today?	IBM X-Force Exchange in QRadar.
77	Section 7.1 Pg. 28	What are your average SIEM Offenses per month?	30 - 70
78	Section 7.1 Pg. 28 Section 9.3 Pg. 33	How many SIEM Use Cases do you have in place today and how many more need to be developed?	100 or more use cases are enabled in QRadar's rules. The number of custom use cases needed is unknown.
79	Section 9.7 Pg.: 33 Table 5 Pg. 31	Section 9.7 indicates "*Vendor is not responsible for hardware, software licenses, or vendor maintenance support for any devices unless specifically set forth in this SOW.*". How can the Vendor be responsible for the system availability?	Vendor is not responsible for licenses or vendor maintenance support of DOR equipment. The vendor is responsible for the hardware, software licenses, or maintenance support of their equipment.
80	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	What is the size of your IT Team?	13
81	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How Many Laptops/Desktops do you have in scope of security monitoring?	3000
81	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How Many Servers do you have in scope of security monitoring (Separate by Windows, Linux etc.)?	500 Windows 200 Linux

Qstn	Citation	Vendor Question	State's Response
83	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How many Network devices do you have in the Network?	120
84	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Do you have infrastructure hosted in the cloud (AWS, Azure, GCP, etc.)?	Azure
85	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Approximately how many security alerts do you and your team receive per day?	Currently, QRadar does not trigger alerts. Palo Alto Firewalls - ~20 or more per day Cortex XDR - ~3 per day FireEye - ~1 or none per day
86	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Do you have Incident Response Plan in place or do we need to come up with one as part of this MDR services?	Yes. There is an Incident Response Plan.
87	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How many events (system events/syslog's/FW logs, etc.) per second/day are we looking at?	Currently, QRadar averages ~17,000 EPS. Day-to-day varies. Other tools outside of QRadar are unknown.
88	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	What anti-virus / malware detection do you use on endpoints (if any)?	Palo Alto Traps. It does not log to QRadar
89	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Who is maintaining the current SIEM infrastructure?	NCDOR
90	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Is QRADAR Fully deployed and Configured at this point?	Yes
91	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	In case QRADAR is not deployed, can we propose alternative SIEM solutions such as LogRhythm / Rapid7 fully managed and implemented MDR solution?	No
92	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	What kind(s) of IDS/IPS do you have?	Palo Alto, FireEye

Qstn	Citation	Vendor Question	State's Response
93	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How many Log sources do you have today in the Network?	642
94	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	What Log aggregator is being used currently for all SIEM logs?	QRadar
95	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	How many DHCP and DNS servers (total) do you have?	18 DHCP servers. DNS Servers do not log to QRadar.
96	Attachment A: Scope of Work Section 7 – Specific Requirements Pages 28-31	Is there a team today looking at the events and working on remediating them actively?	Yes
97	Page 26, Attachment A – SCOPE OF WORK section "This is purely a services model with a shared pool of resources to manage the SIEM and network incidents; this is not a dedicated nor hybrid model of support."	Please clarify the difference between "shared pool" and "hybrid model" here. We assume this means that the vendor will simply supply a pool of resources to support the overall effort, i.e. "co-management" or "managing together" where NCDOR maintains full control of the SIEM environment.	The vendor will supply a pool of resources to support the overall effort, i.e. co-management or management together, where NCDOR maintains full control of the SIEM environment. Remediation is defined as Tier 1 and Tier 2 eyes on the glass. The vendor will not have access to NCDOR security and network tools.
98	Page 26, Attachment A – SCOPE OF WORK section Reference to NCDOR's existing QRadar platform/implementation	Will NCDOR consider the option of using a more widely supported, more cost effective, and interoperable SIEM platform to replace QRadar?	No
99	Page 5, 2.3. OFFER SUBMITTAL Offer must be submitted on the forms provided herein. If additional sheets are required (for example, Vendors who are offering alternate proposals);	Can NCDOR please provide guidelines regarding which parts of this RFP where alternate solutions would be considered? For example, would an alternate SIEM platform be considered if presented?	See response to Question 98 above. However, DOR will consider alternative solutions that integrate into QRadar.

Qstn	Citation	Vendor Question	State's Response
100	Page 26, Attachment A - provide monitoring and remediation support for NCDOR's QRadar SIEM instance and/or network detection devices as a managed service with shared Virtual Security Operations Center (vSOC) resources to support	Is the expectation that the vendor will support the SIEM only or additional network monitoring devices like IPS/Firewalls/HIDS as well? Can you provide additional clarification on the number of devices besides the SIEM that will require support?	Support the SIEM and perform additional network monitoring. DOR will support its own firewalls and network monitoring devices. Remediation is defined as Tier 1 and Tier 2 eyes on the glass. The vendor will not have access to NCDOR security and network tools. 120
101	Page 26, Attachment A – QRADAR current environment	How large is the current deployment of QRADAR today? How many GB/day of logs are being collected? Is there a list of the log sources/type (AD/Firewall/Endpoint) and qty's that are being monitored?	1 All-in-one console, 1 data node, and 1 virtual event collector Average EPS per day is currently 17,000. The amount in GB currently cannot be determined. Yes, QRadar's log sources are displayed with the log source type and the list can be exported.
102	Page 26, Attachment A – RACI Chart	The services that are being requested include monitoring as well administration and tuning of the current system. Are there runbook and use cases implemented inside the system today?	No
103	Page 26, Attachment A – Ticketing Integration and Response	Do you have any type of integration between your SIEM and a ticket/case management system today like ServiceNow, Remedy, etc.?	No. We have ServiceNow in house but it is not currently integrated with our SIEM.
104	Page 26, Attachment A – Use Cases and Runbooks	Depending on the complexity of the configuration and quantity of the runbook and use cases required along with the current configuration of the QRADAR implementation additional blocks of engineering time could be required. Is it safe to assume that we can provide time and materials blocks of hours for additional unforeseen architectural and engineering work that will need to be provided as part of this project?	Vendor may provide time and material blocks of hours for additional unforeseen architectural and engineering work that will need to be provided as part of this project. See Modification 1 (M1) to the IFB on pages1-3.
105	Threat Intelligence Feeds	Do you currently consume any paid or free sources of threat intelligence into your SIEM platform today?	Yes IBM X-Force Exchange

Qstn	Citation	Vendor Question	State's Response
106	SOAR Platform	Do you currently have any SOAR capability in the solution today? Is that in scope for this engagement?	No No
107	Incident Response	Will incident response include emergency as well as non-emergency incident response and remediation? What type of SLA do you require today for emergency incidents? Do you require onsite personnel or will remote IR teams and response be sufficient in this model?	Yes See Attachment A—Scope of Work, Section 7.4. Remote teams are sufficient.
108	Remediation	Will you require remediation support on endpoints, servers, firewalls, etc. in addition to SIEM analysts?	No
109	4.0 Furnish and delivery	SOC Infrastructure is housed within IBM Cloud (SOC2 certified) and would be the only method of connecting to the NC QRadar Console from this physically secure location, which uses a private, single tenant, virtualized desktop. In this SOC architecture, would staff also be required to be in their own distinct physically secured area?	Yes
110	4.0 Furnish and delivery	A subset of the SOC infrastructure could be provided from an IBM Cloud FedRAMP facility if required. Will there be time allotted to allow for this provisioning and documentation?	See M1 above regarding FedRAMP certification.

Failure to acknowledge receipt of this addendum <u>will</u> result in rejection of the response. (UPLOAD Addendum Response to NCBids w/Title Addendum 1)

Check ONE of the following options:

☐ Bid has not been uploaded to NCBids. Any changes resulting from this addendum are included in our response.

☐ Bid has been uploaded to NCBids. No changes resulted from this addendum.

☐ Bid has been uploaded to NCBids. Changes resulting from this addendum are as follows (attach updated documents with Addendum Response:

Execute Addendum:

Offeror: _____

Authorized Signature: _____

Name and Titled (Typed): _____

Date: _____