For: RFP 2024-080 New Hampshire Police Standards and Training Council LMS RMS RFP

Addendum #1 To RFP # 2024-080

1. **Delete Table B-2.2 in its entirety and replace with the following:**

Table B-2.2 Technical Requirements

TECHNICAL REQUIREMENTS					
State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
Prohibited Technologies					
	No equipment or services on the State of New Hampshire's Prohibited Technologies List found here: https://www.doit.nh.gov/sites/g/files/ehbemt506/files/inline-documents/sonh/prohibited-technologies.pdf and No equipment or services on the FCC Covered List found here: https://www.fcc.gov/supplychain/coveredlist	M			
Security Compliance Requirements					
T1.1	Comply with controls required by NIST Special Publication 800-171 R2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations to achieve the Baseline SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC (nist.gov)	M			
T1.2	Comply With Moderate level controls as defined by NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations - BaseLine Plus SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)	P			
StateRAMP Authorization					
T2.1	StateRAMP Ready/Authorized Certification Home - StateRAMP	P			

T2.2	If StateRAMP Ready, you agree to attain StateRAMP Authorized within 12 months of the effective date of a resulting contract.	M			
T2.3	If StateRAMP Active, you agree to attain StateRAMP Authorized within 24 months of the effective date of a resulting contract.	M			
T2.4	If StateRAMP In Process, you agree to attain StateRAMP Authorized within 24 months of the effective date of a resulting contract.	M			
T2.5	If StateRAMP Pending (Under review with StateRAMP PMO awaiting a determination for a verified status), you agree to attain StateRAMP Authorized within 24 months of the effective date of a resulting contract or prior to contract renewal.	M			
T2.6	If Not StateRAMP Progressing, Not StateRAMP Ready, or Not StateRAMP Authorized the vendor shall initiate and provide a StateRAMP Security Snapshot with their response. You agree to attain StateRAMP Authorized within 24 months of the effective date of a resulting contract.	M			
T2.7	Continuous Monitoring – For any resulting award(s) and subsequent contract(s), the awarded contractor(s) will grant access to continuous monitoring and reporting upon receiving award for StateRAMP Security Snapshot, Ready status and Authorization status through the life of the contract. The State reserves the right to request and review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor's environment. The contractor shall respond to all flaws discovered by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.	M			
Other Certifications in lieu of StateRAMP					
T3.1	FedRAMP Authorized How to Become FedRAMP Authorized | FedRAMP.gov	P			
T3.2	HITRUST (HITRUST is common for Health Care related products and services.) HITRUST Alliance | Information Risk Management and Compliance	P			
Hosted Platform					

T4.1	The following Hosting Platforms are FedRAMP/StateRAMP Authorized and are pre-approved to host any SaaS or other Software Product. If your platform is included in the list below identify the platform in the Vendor Comments. • AWS US East/West • AWS GOVCLOUD • AZURE Commercial Cloud • AZURE Government (Includes Dynamics 365) • GOOGLE Services (Cloud Platform Products and Underlying Infrastructure) • ORACLE Government Cloud – Common Controls • ORACLE Federal Managed Cloud Services	P			
Individual Agency Compliance Requirements (examples listed below)					
T5.1	FTI Pub 1075	M			
T5.2	HIPAA	M			
T5.3	FERPA	M			
T5.4	CIJS	M			
Information Technology Accessibility Compliance					
T6.1	Web content and mobile applications must comply with WCAG 2.1, Level AA.	M			
T6.2	Hardware that transmits information or has a user interface, such as display screens, variable message signs, and kiosks, must comply with ICT Accessibility Standards and Guidelines, Chapter 4: Hardware.	M			
T6.3	Vendor shall complete the VPAT 2.5 WCAG (November 2023) and submit with their proposal in Section III: Responses to Requirements and Deliverables https://www.itic.org/policy/accessibility/vpat	M			

2. Delete Section B-2.3 in its entirety (Statewide Technical Requirements - Statewide Information Security Manual (SISM))