STATE OF NEW HAMPSHIRE

Department of Safety:
RFP DOS 2027-01
NH Sex Offender Registry Public Website

RFP ISSUED	9/30/2026
VENDOR CONFERENCE (Optional)	10/27/2026
LOCATION	Virtual
STATE AGENCY POINT OF CONTACT	Name: Dianna Courtemanche email: DOSContracts@dos.nh.gov Tel: 603-223-8000, Option 8
PROPOSAL DUE DATE	12/16/2026; 2:00 PM ET

Table of Contents

SECTION 1: OVERVIEW AND SCHEDULE OF EVENTS 3
SECTION 2: PROPOSAL SUBMISSION, DEADLINE, AND LOCATION INSTRUCTIONS 5
SECTION 3: PROPOSAL ORGANIZATION, CONTENT, AND REQUIRED ITEMS 7
SECTION 4: EVALUATION OF PROPOSALS 11
SECTION 5: TERMS AND CONDITIONS RELATED TO THE RFP PROCESS 16
SECTION 6: CONTRACT TERMS AND AWARD 20
APPENDIX A: VENDOR CONFERENCE REQUIREMENTS 22
APPENDIX B: BUSINESS/TECHNICAL REQUIREMENTS AND DELIVERABLES 23
APPENDIX C: TOPICS FOR MANDATORY RESPONSES 36
APPENDIX D: STANDARDS FOR DESCRIBING VENDOR QUALIFICATIONS 52
APPENDIX E: PRICING 54
APPENDIX F: DOIT INFRASTRUCTURE AND SECURITY 60
APPENDIX G: MERCHANT CARD SERVICES 62
APPENDIX H: TERMS AND DEFINITIONS 64
APPENDIX I: P-37 STATE OF NEW HAMPSHIRE GENERAL PROVISIONS AND EXHIBITS 68

Remainder of this page intentionally left blank

SECTION 1: OVERVIEW AND SCHEDULE OF EVENTS

1. Executive Summary

1.1. Introduction

The Sex Offender Registry's (SOR) primary responsibility is to maintain the database of sex offenders within the State of New Hampshire. Upon an offender's conviction, personnel assigned to the Unit will receive the criminal record, police reports and court documents to confirm the conviction, which in turn determines the appropriate Tier for each offender to be assigned. Unit personnel provide information to the local police departments on new offenders, so they can complete their required initial and subsequent registrations. Offenders register with their local police departments on a semi-annual or quarterly basis and that information is forwarded to the State Police for updates when necessary. Offenders are also required to report in person to the police department if they make a change to their name, address, employer, or school. Any other changes they make to the required reporting i.e.: on-line identifiers, vehicle information and phone numbers can be done through the mail. The SOR's public website is updated on a weekly basis with the information taken directly from our SOR database. This information includes a current warrant list, as well as any information available on offenders against children, (Megan's Law), and any offenders with multiple criminal episodes. The website includes photographs of each of the offenders that are available to the public. They are also required to report any changes to their personal information including temporary addresses, personal descriptors, vehicles, phone numbers, email accounts, and travel information. This information is collected on the registration form and sent into the SOR Unit for daily updates that staff enter into the database manually. Unit personnel in the SOR processed over 11,795 registration forms during the 2023 calendar year.

The Department of Safety, Division of State Police, is responsible for maintaining and administering the Sex Offender Registry program, supporting statutory compliance processes, and publishing lawful public-facing registry information.

Project Overview/Justification: – The Department seeks a vendor solution to modernize the public Sex Offender Registry website and related administrative capabilities, including public search, mapping, FAQ content, tip/comment intake, annual fee payment support, and reporting/audit capabilities tied to public publication and payment administration.

- Improve public access to lawful registry information through a searchable, map-enabled, mobile-responsive website.
- Reduce manual effort by implementing at least daily automated publication of approved public registry data from the authoritative source.
- Strengthen administrative oversight through audit logging, reporting, role-based access, exception handling, and document management.

No equipment or services on the State of New Hampshire's Prohibited Technologies List found here: Prohibited Technologies List and No equipment or services on the FCC Covered List found here: FCC Section 2 List of Equipment and Services

2. Schedule of Events

The following table provides a Schedule of Events for this RFP through contract finalization and approval. The Agency reserves the right to amend this Schedule at its sole discretion and at any time through a published Addendum.

EVENT	DATE & TIME (ET)
RFP Released to Vendors/Inquiry Period Begins (on or about)	09/30/2026
Notification to the State of the Number of Representatives Attending the Vendor Conference (Optional)	10/07/2026
Vendor Conference (Optional)	Virtual-10/27/2026
Vendor Inquiry Period Ends (Final Inquiries due)	11/13/2026
Final State Responses to Vendor Inquiries	11/30/2026
Final Date and Time for Proposal Submission	12/16/2026 2:00 PM ET
Invitations for Oral Presentations	12/28/2026
Vendor Presentations/Discussion Sessions/Interviews (Mandatory)	Week of 01/04/2027
Estimated Date of Vendor Selection	TBD
Anticipated Governor and Council Approval	TBD

Remainder of this page intentionally left blank

SECTION 2: PROPOSAL SUBMISSION, DEADLINE, AND LOCATION INSTRUCTIONS

1. Proposal Submission

Electronic Proposals submitted in response to this RFP must be received no later than the time and date specified in the Schedule of Events, herein.

The Price Proposal must be labeled clearly and submitted separately from the Technical Proposal.

Late submissions will not be accepted. Delivery of the Proposals shall be the Vendor's responsibility. The time of receipt shall be considered when a Proposal has been officially documented by the Agency, in accordance with its established policies, as having been received via email as designated below. The Agency accepts no responsibility for damaged, mislabeled, or undeliverable emailed Proposals.

2. Electronic Proposals

Electronic Proposals must be addressed to:

TO: DOSContracts@dos.nh.gov

Proposals must be clearly marked as follows:

Subject: RESPONSE TO RFP: RFP DOS 2027-01 NH Sex Offender Registry Public Website

Electronic Submissions must be submitted using the following criteria:

Searchable PDF Format

Files must be less than 10MB in size.

Exception: If files are greater than 10MB in size, the Vendor will be required to submit their Proposal in parts. It is the Vendor's responsibility to ensure a complete Proposal is submitted.

Electronic Submissions shall include:

Attachment 1: Technical Proposal:

a) The Technical Proposal, including all required attachments.
b) One (1) copy of the Proposal Transmittal Form Letter (described in Section 3.1.2: Transmittal Form Letter, herein) shall be signed by an official authorized to legally bind the Vendor and shall be marked "ORIGINAL."

Attachment 2: Price Proposal:

a) The Price Proposal must be labeled clearly and separate from the Technical Proposal.
b) The Price Proposal must include the Pricing Worksheets (as described in Appendix E).

3. Number of Proposals

Vendors may submit one (1) proposal in response to this RFP. Each proposal must identify a single primary hosting model (Vendor-hosted/cloud or State-hosted/on-premises) and a proposed solution.

The State is intentionally accepting both Vendor-hosted/cloud and State-hosted/on-premises Solutions. Vendors shall identify one primary hosting model and proposed Solution in their Proposal. The State will evaluate the proposed Solution based on the requirements and evaluation criteria applicable to that hosting model.

A Vendor's disclosure or distribution of its Proposal other than to the State will be grounds for disqualification.

4. Vendor Inquiries

All inquiries concerning this RFP, including but not limited to, requests for clarifications, questions, and any changes to the RFP, shall be submitted via email to the following RFP Point of Contact:

Dianna Courtemanche

Email: DOSContracts@dos.nh.gov

Inquiries must be received by the RFP Point of Contact no later than the conclusion of the Vendor Inquiry Period identified in the Schedule of Events. Inquiries received later than the conclusion of the Vendor Inquiry Period shall not be considered properly submitted and may not be considered. The State assumes no liability for assuring accurate/complete email transmission/receipt and is not required to acknowledge receipt.

The Agency intends to issue official responses to properly submitted inquiries on or before the date specified in the Schedule of Events section, herein. The Agency may consolidate and/or paraphrase questions for sufficiency and clarity. Oral statements, representations, clarifications, or modifications concerning the RFP shall not be binding upon the Agency. Official responses by the Agency will be made only in writing by the process described above.

The Agency will require the selected Vendor to execute a Contract using the P-37 State of New Hampshire General Provisions and any attached exhibits. To the extent that a Vendor believes that exceptions to the standard form contract will be necessary for the Vendor to enter into the Agreement, the Vendor must submit those exceptions during the Vendor Inquiry Period.

5. Restriction of Contact with Agency Employees

From the date of release of this RFP until an award is made and announced regarding the selection of a Vendor, all communication with personnel employed by or under contract with the Agency regarding this RFP is prohibited unless first approved by the RFP Points of Contact listed herein. Agency employees have been directed not to hold conferences and/or discussions concerning this RFP with any potential Contractor during the selection process, unless otherwise authorized by the RFP Point of Contact. Vendors may be disqualified for violating this restriction on communications.

6. Validity of Proposal

Proposals must be valid for one hundred and eighty (180) days following the deadline for submission of Proposals in the Schedule of Events, or until the Effective Date of any resulting Contract, whichever is later.

SECTION 3: PROPOSAL ORGANIZATION, CONTENT, AND REQUIRED ITEMS

1. Proposal Organization

Proposals should adhere to the following outline:

Cover Page

Transmittal Form Letter

Table of Contents

Section I: Executive Summary

Section II: Glossary of Terms and Abbreviations

Section III: Responses to Requirements and Deliverables

Section IV: Narrative Responses

Section V: Corporate Qualifications

Section VI: Qualifications of Key Vendor staff

Section VII: Vendor Attachments

Section VIII: Price Proposal (separate file from the Technical Proposal)

1.1. Cover Page

The first page of the Vendor's Proposal should be a cover page containing the following text:

STATE OF NEW HAMPSHIRE

Department of Safety

RESPONSE TO RFP: RFP DOS 2027-01 NH Sex Offender Registry Public Website

The cover page should also include the Vendor's name, contact person, contact telephone number, address, city, state, zip code, and email address.

1.2. Transmittal Form Letter

The Vendor must submit a signed Transmittal Form Letter with their response using the Transmittal Form Letter template provided on the following page. Any electronic alteration to the content of this Transmittal Form Letter template is prohibited. Any such changes shall result in a Proposal being rejected.

State of New Hampshire Proposal Transmittal Form Letter

Company Name:
Address:
To: Dianna Courtemanche
DOSContracts@dos.nh.gov

RE: Proposal Invitation Name: NH Sex Offender Registry Public Website
Proposal Number: RFP DOS 2027-01
Proposal Due Date and Time: 12/16/2026; 2:00 PM EST

To Whom It May Concern:
Company Name: _____ hereby submits an offer to provide to the State of New Hampshire the Services indicated in NH Sex Offender Registry Public Website RFP DOS 2027-01 at the price(s) quoted in Vendor Response Section VIII: Price Proposal, in complete accordance with all conditions of this RFP and all Specifications set forth in the RFP and in the P-37 State of New Hampshire General Provisions and Exhibits, identified in Appendix I.

We attest to the fact that:

1. The company has reviewed and agreed to be bound by the RFP.
2. The company has not altered any of the language or other provisions contained in the RFP document.
3. The Proposal is effective for a period of 180 days from the RFP Closing Date or until the Effective Date of any resulting Contract, whichever is later.
4. The prices quoted in the Proposal were established without collusion with other vendors.
5. The Vendor has read and fully understands this RFP.

Further, in accordance with RSA 21-I:11-c, the undersigned Vendor certifies that neither the Vendor nor any of its subsidiaries, affiliates or principal officers (principal officers refers to individuals with management responsibility for the entity or association):

a) Has, within the past 2 years, been convicted of, or pleaded guilty to, a violation of RSA 356:2, RSA 356:4, or any state or federal law or county or municipal ordinance prohibiting specified bidding practices, or involving antitrust violations, which has not been annulled.
b) Has been prohibited, either permanently or temporarily, from participating in any public works project pursuant to RSA 638:20.
c) Has previously provided false, deceptive, or fraudulent information on a vendor code number application form, or any other document submitted to the state of New Hampshire, which information was not corrected as of the time of the filing a bid, proposal, or quotation.
d) Is currently debarred from performing work on any project of the federal government or the government of any state.
e) Has, within the past 2 years, failed to cure a default on any contract with the federal government or the government of any state.
f) Is presently subject to any order of the department of labor, the department of employment security, or any other state department, agency, board, or commission,

finding that the applicant is not in compliance with the requirements of the laws or rules that the department, agency, board, or commission is charged with implementing.

g) Is presently subject to any sanction or penalty finally issued by the department of labor, the department of employment security, or any other state department, agency, board, or commission, which sanction or penalty has not been fully discharged or fulfilled.
h) Is currently serving a sentence or is subject to a continuing or unfulfilled penalty for any crime or violation noted in this section.
i) Has failed or neglected to advise the division of any conviction, plea of guilty, or finding relative to any crime or violation noted in this section, or of any debarment, within 30 days of such conviction, plea, finding, or debarment: or
j) Has been placed on the debarred parties list described in RSA 21-I:11-c within the past year.

This document shall be signed by a person who is authorized to legally obligate the responding Vendor. A signature on this document indicates that all State of New Hampshire terms and conditions are accepted by the responding Vendor and that any and all other terms and conditions submitted by the responding Vendor are null and void, even if such terms and conditions have terminology to the contrary. The responding Vendor shall also be subject to State of New Hampshire terms and conditions as stated on the reverse of the purchase order, if any.

Our official point of contact is:
Title: _____

Telephone: _____

Email: _____

Authorized Signature Printed: _____

Authorized Signature: _____

1.3. Table of Contents

The Vendor must provide a table of contents with corresponding page numbers relating to its Proposal.

1.4. Section I: Executive Summary

Section I shall provide an executive summary, not to exceed two (2) pages, identifying how the Vendor satisfies the goals of this RFP. The executive summary will also provide an overview of the Vendor's proposed Solution and Services highlighting those factors that they believe distinguish their Proposal.

1.5. Section II: Glossary of Terms and Abbreviations

Section II shall provide a glossary of all terms, acronyms, and abbreviations used in the Vendor's Proposal.

1.6. Section III: Responses to System Requirements and Deliverables

Section III shall include the response tables from the Business/Technical Requirements and Deliverables Appendix. The Vendor must document the ability to meet the Business Requirements, Technical Requirements and Deliverables of this RFP.

1.7. Section IV: Narrative Responses

Section IV solicits narrative responses describing the Software, Technical, Services and Project Management topics defined for this RFP Project. The Topic for Mandatory Responses Appendix is organized into sections, which correspond to the different aspects of the scoring process of the Proposal. Discussion of each topic must begin on a new page.

1.8. Section V: Corporate Qualifications

Section V shall provide the corporate qualifications of the Vendor, and any Subcontractors proposed to participate in the Project. Specific information to be provided is described in the Standards for Describing Vendor Qualifications Appendix.

1.9. Section VI: Qualifications of Key Vendor Staff

Section VI shall be used to provide required information on the Vendor's Key Project Staff. Specific information to be provided is described in the Standards for Describing Vendor Qualifications Appendix.

1.10. Section VII: Vendor Attachments

Section VII provides for extra materials as referenced in the Topic for Mandatory responses Appendix such as Product Literature, Ad Hoc/Federal Reporting, Interface Standards, Testing (For UAT Plan) and Status Meetings and Reports.

1.11. Section VIII: Price Proposal (separate file from the Technical Proposal)

Section VIII shall include the Price Proposal, which must describe the proposed price of the Vendor Proposal based on and reflected by the inclusion of the completed tables listed in the Pricing Appendix. As outlined in Section 2: Proposal Submission, Deadline, and Location Instructions, this price proposal must be labeled clearly and sealed separately from the Technical Proposal.

SECTION 4: EVALUATION OF PROPOSALS

1. Criteria for Evaluation and Scoring

Each responsive Proposal will be evaluated and considered with regard to the Solution and Services proposed, qualifications of the Vendor and any Subcontractors, experience and qualifications of proposed candidates, and price.

If the Agency determines to make an award, the Agency will begin negotiations with a Vendor based on these evaluations. Should the Agency be unable to reach agreement with the high scoring Vendor during Contract discussions, the Agency may then undertake Contract discussions with the next high scoring Vendor and so on; or the Agency may reject all Proposals, cancel this RFP, or solicit new Proposals under a new acquisition process.

The Agency will use a scoring scale of one thousand (1000) Points. Points will be distributed as set forth in the table below.

Table 4.1: Scoring of Proposal

CATEGORIES	**POINTS**
Technical Proposal with the following potential maximum scores for each Technical Proposal category listed below:	**600**
Proposed Solution	310
Vendor's Technical, Service and Project Management Experience	100
Vendor Company	50
Staffing Qualifications	50
Security, Compliance, and Hosting Assurance	90
Price Proposal Potential Maximum Points	**400**
TOTAL POTENTIAL MAXIMUM POINTS AWARDED	one thousand (1000)

The Agency will select a Vendor based upon the criteria and standards contained in this RFP and from applying the weighting in this section. Oral interviews and reference checks, to the extent they are utilized by the Agency, will be used to refine and finalize technical scores.

2. Scoring Detail

2.1. Scoring of the Proposed Solution

The Vendor's Proposed Solution will be allocated a maximum score of 310 Points. The main purpose of this section is to measure how well the Solution meets the business needs of the Agency.

Scoring is primarily measured using vendor responses in the following sections:

a) Proposal Section III: Responses to Requirements and Deliverables

b) Proposal Section IV: Narrative Responses

c) Vendor Presentation and Demonstration (Mandatory)

2.2. Scoring of Vendor Technical, Service, and Project Management Experience

Vendor proposed Technical, Service, and Project Management Experience will be allocated a maximum score of 100 Points. In this section, the State will score the technical merits of how the Vendor will carry out the Implementation and maintenance of the Solution. Technical details of the System including security and protection of data, proposed training administrative procedures, how the Vendor manages its team and the Project will be critical. How compatible the Vendor's procedures and technologies are with the State contribute to an assessment of risk both in the short and long term.

Scoring is primarily measured using vendor responses in the following sections:

a) Proposal Section III: Responses to Requirements and Deliverables

b) Proposal Section IV: Narrative Responses

c) Proposed Work Plan

d) References

2.3. Scoring of Vendor Company

Vendor Company qualifications will be allocated a maximum score of 50 points. It must be established that the Vendor Company is capable of carrying out the Project through Implementation, the Warranty Period and the maintenance period.

Scoring is primarily measured using vendor responses in the following sections:

a) Proposal Section V: Corporate Qualifications

b) References

2.4. Scoring of Vendor Staffing Qualifications

Vendor's Staff qualifications will be allocated a maximum score of 50 points. Vendor's Staff must have the training and experience to support the Vendor's plans to implement and support the System.

Scoring is primarily measured using vendor responses in the following sections:

a) Proposal Section VI: Qualifications of Key Staff

b) Vendor Presentations & Demonstrations (Mandatory)

c) References

2.5. Security, Compliance, and Hosting Assurance.

The Vendor's Security, Compliance, and Hosting Assurance will be allocated a maximum score of ninety (90) points.

The State will evaluate the security, compliance, and hosting characteristics of the proposed Solution based on the proposed hosting model. Both Vendor-hosted and State-hosted/on-premises Solutions are eligible to receive the full ninety (90) points. The State will not award points solely based on the proposed hosting model.

For Vendor-hosted Solutions, the State may consider the Vendor's FedRAMP, GovRAMP, or other applicable independent security authorization or assessment, the security of the proposed hosting environment, the security of the proposed application, and the Vendor's ability to maintain the required security posture throughout the Contract term.

For State-hosted or on-premises Solutions, the State will evaluate the proposed security architecture, applicable security controls, access controls, vulnerability and patch management, logging and monitoring, data protection, backup and recovery, incident response, and other applicable security measures associated with the proposed Solution.

GovRAMP authorization is a significant security assurance factor for applicable Vendor-hosted Solutions. A Vendor-hosted Solution that is fully FedRAMP or GovRAMP Authorized and within the applicable authorization period may receive the maximum points available for the applicable security assurance component. However, GovRAMP authorization is not applicable to a State-hosted or on-premises Solution and shall not, by itself, result in a scoring advantage or disadvantage for a Solution based solely on its hosting model.

The State will consider the following, as applicable to the proposed hosting model:

a) Security architecture and implementation;

b) Compliance with applicable State security requirements and standards;

c) FedRAMP or GovRAMP status, where applicable;

d) Independent security assessments, certifications, audits, or other objective evidence of security controls;

e) Protection of State data, including encryption, access control, data handling, and data location;

f) Vulnerability management, security testing, patching, and remediation;

g) Security logging, monitoring, alerting, and incident response;

h) Backup, recovery, disaster recovery, and business continuity;

i) Physical and environmental security of the hosting environment, where applicable; and

j) The overall effectiveness and maturity of the proposed security and compliance approach.

The State reserves the right to request supporting documentation, including security assessment reports, audit reports, certifications, authorization documentation, penetration testing results, vulnerability assessments, policies, procedures, and other evidence necessary to evaluate the proposed Solution.

Scoring will be based on the quality, completeness, applicability, and demonstrated effectiveness of the Vendor's proposed security and compliance approach.

2.6. Scoring the Price

The Vendor's price will be allocated a maximum score of 400 points. The State will only consider Pricing provided in Appendix E - Pricing Tables E-1.1 through E-1.7 The price information required in a Proposal is intended to provide a sound basis for comparing price. The Vendor's Price Score formula described in the Price Proposal Review and Scoring section will be utilized for this scoring portion.

3. Planned Evaluations

The Agency plans to use the following process:

a) Initial screening to ensure that the Proposals are in compliance with submission requirements.
b) Preliminary evaluation of the Proposals.
c) Oral interviews and Product Demonstrations (if applicable).
d) Final Evaluation of Technical Proposals and scoring.
e) Review of Price Proposals and scoring.
f) Select the highest scoring Vendor and begin contract negotiation.

3.1. Initial Screening

The Agency will conduct an initial screening step to verify Vendor compliance with the submission requirements set forth in the RFP and the minimum content set forth in the Proposal Format, Content and Required Items within this RFP. The Agency may waive or offer a limited opportunity to cure immaterial deviations from the RFP requirements if it is determined to be in the best interest of the State. A Proposal that fails to satisfy either submission requirements or minimum standards may be rejected without further consideration.

3.2. Preliminary Technical Scoring of Proposals

The Agency will establish an evaluation team. This evaluation team will review the Technical Proposals and give a preliminary score. Should a Vendor fail to achieve 400 minimum points in the preliminary scoring, it will receive no further consideration from the evaluation team and the Vendor's Price Proposal will remain unopened. Price Proposals will remain unopened during the preliminary technical review, Oral Interviews and Product Demonstrations.

3.3. Oral Interviews and Product Demonstrations

At the Agency's discretion, Vendors may be invited to oral interviews and/or product demonstrations including demonstrations of any proposed automated systems or technology components. The Agency retains the sole discretion to determine whether to conduct oral interviews and product demonstrations, with which Vendors, the number of interviews and the length of time provided for the interview and Product demonstration. The Agency may decide to conduct oral interviews and product demonstrations with less than all responsive Vendors.

The purpose of oral interviews and product demonstrations is to clarify and expound upon information provided in the written Proposals. Vendors are prohibited from altering the basic substance of their Proposals during the oral interviews and product demonstrations. The Agency may ask the Vendor to provide written clarifications of elements in their Technical Proposal regardless of whether it intends to conduct oral interviews.

Information gained from oral interviews and product demonstrations will be used to refine technical review scores assigned from the initial review of the Proposals. All costs associated with oral presentations/interviews shall be borne entirely by the Vendor.

3.4. Final Scoring of Technical Proposals

Following Oral Interviews, Product Demonstrations, Reference Checks (if appropriate) and/or review of written clarifications of Proposals requested by the Agency, the evaluation team will determine a final score for each Technical Proposal.

3.5. Price Proposal Review and Scoring

Price Proposals will be reviewed upon completion of the final scoring of Technical Proposals. The Vendor's Price Proposal will be allocated a maximum potential score of 400 points. Vendors are advised that this is not a low bid award and that the scoring of the price Proposal will be combined with the scoring of the Technical Proposal to determine the overall highest scoring Vendor.

The following formula will be used to assign points for Price:

Vendor's Price Score = (Lowest Proposed Price / Vendor's Proposed Price) x Maximum Number of Points for Price Proposal.

For the purpose of use of this formula, the lowest proposed price is defined as the lowest price proposed by a Vendor who has scored above the minimum necessary for consideration on the Technical Score.

4. No Best and Final Offer

The Proposal should be submitted initially on the most favorable terms that the Vendor can offer. There will be no best and final offer procedure. The Vendor should be prepared to accept this RFP for incorporation into a contract resulting from this RFP. Contract negotiations may incorporate some or the entire Proposal.

5. Rights of the Agency in Accepting and Evaluating Proposals

The Agency reserves the right to:

a) Make independent investigations in evaluating Proposals.

b) Request additional information to clarify elements of a Proposal.

c) Waive minor or immaterial deviations from the RFP requirements, if determined to be in the best interest of the State.

d) Omit any planned evaluation step if, in the Agency's view, the step is not needed.

e) At its sole discretion, reject any and all Proposals at any time.

f) Open contract discussions with the second highest scoring Vendor and so on, if the Agency is unable to reach an agreement on Contract terms with the higher scoring Vendor(s).

SECTION 5: TERMS AND CONDITIONS RELATED TO THE RFP PROCESS

1. RFP Addendum

The Agency reserves the right to amend this RFP at its discretion, prior to the Proposal submission deadline. In the event of an addendum to this RFP, the Agency, at its sole discretion, may extend the Proposal submission deadline, as it deems appropriate.

2. Non-Collusion

The Vendor's signature on a Proposal submitted in response to this RFP guarantees that the prices, terms and conditions, and Work quoted have been established without collusion with other Vendors and without effort to preclude the Agency from obtaining the best possible competitive Proposal.

3. Property of the State

All material received in response to this RFP shall become the property of the State and will not be returned to the Vendor. Upon Contract award, the State reserves the right to use any information presented in any Proposal.

4. Confidentiality of a Proposal

The substance of a Proposal must remain confidential until the Effective Date of any Contract resulting from this RFP. A Vendor's disclosure or distribution of Proposals other than to the Agency without the Agency's prior consent may be grounds for disqualification.

5. Public Disclosure

In general, the State is obligated to make public the information submitted in response to this RFP (including all materials submitted in connection with it, such as attachments, exhibits, addenda, and presentations), any resulting contract, and information provided during the contractual relationship. The Right-to-Know law (RSA 91-A) obligates the State to conduct an independent analysis of the confidentiality of the information submitted, regardless of whether it is marked confidential.

In addition, the Governor and Council (G&C) contract approval process more specifically requires that pricing be made public and that any contract reaching the G&C agenda for approval be posted online.

5.1. Disclosure of Information Submitted in Response to RFP

Information submitted in response to this RFP is subject to public disclosure under the Right-to-Know law after the award of a contract by G&C. At the time of closing date for Proposals, the State will post the number of responses received with no further information. Pursuant to RSA 21-G:37, the State will also post the name and rank or score of each Vendor pursuant to the timeliness requirements therein. Notwithstanding the Right-to-Know law, no information concerning the contracting process, including, but not limited to information related to proposals, communications between the parties or contract negotiations, shall be available until a contract is approved by G&C, or, if the contract does not require G&C approval, until the contract has been actually awarded. This means unsuccessful Vendors shall not be notified of the outcome until that time.

Confidential, commercial, or financial information may be exempt from public disclosure under RSA 91-A:5, IV. If a Vendor believes any information submitted in response to this request for proposal should be kept confidential, the Vendor must specifically identify that information where it appears in the submission in a manner that draws attention to the designation and must mark/stamp each page of the materials that the Vendor claims must be exempt from disclosure as "CONFIDENTIAL." Vendors must also provide a letter to the person listed as the point of contact for this RFP, identifying the specific page number and section of the information you consider to be confidential, commercial or financial and providing your rationale for each designation. Marking or designating an entire proposal, attachment or section as confidential shall neither be accepted nor honored by the State. Vendors must also provide a separate copy of the full and complete document, fully redacting those portions and shall note on the applicable page or pages that the redacted portion or portions are "confidential."

Submissions which do not conform to these instructions by failing to include a redacted copy (if necessary), by failing to include a letter specifying the rationale for each redaction, by failing to designate the redactions in the manner required by these instructions, or by including redactions which are contrary to these instructions or operative law may be rejected by the State as not conforming to the requirements of the proposal.

Pricing, which includes but is not limited to, the administrative costs and other performance guarantees in Proposals or any subsequently awarded contract shall be subject to public disclosure regardless of whether it is marked as confidential.

Notwithstanding a Vendor's designations, the State is obligated under the Right-to-Know law to conduct an independent analysis of the confidentiality of the information submitted in a proposal. If a request is made to the State by any person or entity to view or receive copies of any portion of the proposal, the State shall first assess what information it is obligated to release. The State will then notify you that a request has been made, indicate what, if any, information the State has assessed is confidential and will not be released, and specify the planned release date of the remaining portions of the proposal. To halt the release of information by the State, a Vendor must initiate and provide to the State, prior to the date specified in the notice, a court action in the Superior Court of the State of New Hampshire, at its sole expense, seeking to enjoin the release of the requested information.

By submitting a proposal, Vendors acknowledge and agree that:

The State may disclose any and all portions of the proposal or related materials that are not marked as confidential and/or which have not been specifically explained in the letter to the person identified as the point of contact for this RFP;

The State is not obligated to comply with a Vendor's designations regarding confidentiality and must conduct an independent analysis to assess the confidentiality of the information submitted in your proposal; and

The State may, unless otherwise prohibited by court order, release the information on the date specified in the notice described above without any liability to a Vendor.

Electronic Posting of Resulting Contract

RSA 91-A obligates disclosure of contracts resulting from responses to RFPs. As such, the Secretary of State provides to the public any document submitted to G&C for approval, and posts those documents, including the contract, on its website. Further, RSA 9-F:1 requires that contracts stemming from RFPs be posted online. By submitting a Proposal, Vendors acknowledge and agree that, in accordance with the above-mentioned statutes and policies, (and regardless of whether any specific request is made to view any document relating to this RFP), any contract resulting from this RFP that is submitted to G&C for approval will be made accessible to the public online via the State's website.

6. Non-Commitment

Notwithstanding any other provision of this RFP, this RFP does not commit the Agency to award a Contract. The Agency reserves the right, at its sole discretion, to reject any and all Proposals, or any portions thereof, at any time; to cancel this RFP; and to solicit new Proposals under a new acquisition process.

7. Proposal Preparation Cost

By submitting a Proposal, a Vendor agrees that in no event shall the Agency be either responsible for or held liable for any costs incurred by a Vendor in the preparation of or in connection with the Proposal, or for work performed prior to the Effective Date of a resulting Contract.

8. Ethical Requirements

From the time this RFP is published until a contract is awarded, no vendor shall offer or give, directly or indirectly, any gift, expense reimbursement, or honorarium, as defined by RSA 15-B, to any elected official, public official, public employee, constitutional official, or family member of any such official or employee who will or has selected, evaluated, or awarded an RFP, or similar submission. Any vendor that violates RSA 21-G:38 shall be subject to prosecution for an offense under RSA 640:2. Any vendor who has been convicted of an offense based on conduct in violation of this section, which has not been annulled, or who is subject to a pending criminal charge for such an offense, shall be disqualified from applying to the RFP, or similar request for submission and every such vendor shall be disqualified from applying to on any RFP or similar request for submission issued by any State agency. A vendor that was disqualified under this section because of a pending criminal charge which is subsequently dismissed, results in an acquittal, or is annulled, may notify the Department of Administrative Services (DAS), which shall note that information on the list maintained on the State's internal intranet system, except in the case of annulment, the information, shall be deleted from the list.

9. Debarment

Vendors who are ineligible to apply to proposals, bids or quotes issued by the Department of Administrative Services, Division of Procurement and Support Services pursuant to the provisions of RSA 21-I:11-c shall not be considered eligible for an award under this proposal.

10. Challenges on Form or Process of the RFP

A vendor questioning the Agency's identification of the selected Vendor may request that the Agency review its selection process. Such request shall be made in writing and be received by the Agency within 5 (five) business days after the rank or score is posted on the agency website. The request shall specify all points on which the vendor believes the Agency erred in its process and shall contain such argument in support of its position as the vendor seeks to present. In response, the issuing Agency shall review the process it followed for evaluating responses and, within 5 (five) business days of receiving the request for review, issue a written response either affirming its initial selection of a Vendor or canceling the application. In its request for review, a vendor shall not submit, and an Agency shall not accept nor consider, any substantive information that was not included by the vendor in its original application response. No hearing shall be held in conjunction with a review. The outcome of the Agency's review shall not be subject to appeal.

Remainder of this page intentionally left blank

SECTION 6: CONTRACT TERMS AND AWARD

1. Non-Exclusive Contract

Any resulting Contract from this RFP will be a Non-Exclusive Contract. The State reserves the right, at its discretion, to retain other contractors to provide any of the Services or Deliverables identified under this procurement or make an award by item, part or portion of an item, group of items, or total Proposal.

2. Award

Any resulting Contract is contingent upon approval of the Contract by Governor and Executive Council of the State of New Hampshire and upon continued appropriation of funding for the Contract.

3. Anticipated Contract Term

The Vendor shall be fully prepared to commence work after full execution of the Contract by the parties, and the receipt of required governmental approvals, including, but not limited to, Governor and Executive Council of the State of New Hampshire approval ("Effective Date").

The initial Contract Term will begin on the Effective Date and continue for two years. The Contract Term may be extended twice for up to two years per extension for up to four years total ("Extended Contract Term") at the sole option of the State, subject to the party's prior written agreement on terms and applicable fees for each extended Contract Term, contingent upon satisfactory vendor performance, continued funding and Governor and Executive Council approval, for a total aggregate term of **six years**.

4. Standard Contract Terms

The Agency will require the successful vendor to execute a Contract. The P-37 State of New Hampshire General Provisions and Exhibits, identified in Appendix I will form the basis of any Contract resulting from this RFP.

To the extent that a Vendor believes that exceptions to the standard form Contract will be necessary for the Vendor to enter into the Agreement, the Vendor should note those issues during the Vendor Inquiry Period. The Agency will review requested exceptions and accept, reject or note that it is open to negotiation of the proposed exception at its sole discretion. If the Agency accepts a Vendor's exception the Agency will, at the conclusion of the inquiry period, provide notice to all potential Vendors of the exceptions which have been accepted and indicate that exception is available to all potential Vendors. Any exceptions to the standard form contract that are not raised during the Vendor inquiry period are waived. In no event is a Vendor to submit its own standard contract terms and conditions as a replacement for the State's terms in response to this solicitation.

4.1. Contract Negotiations and Unsuccessful Vendor Notice

If a Vendor is selected, the State will notify the selected Vendor in writing of their selection and the State's desire to enter into contract discussions. Until the State successfully completes discussions with the selected Vendor, all submitted Proposals remain eligible for selection by the State. In the event contract discussions are unsuccessful with the selected Vendor, the evaluation team may recommend another Vendor.

4.2. Subcontractors

The Vendor shall remain wholly responsible for performance of the entire Contract regardless of whether a Subcontractor is used. The State will consider the Vendor to be the sole point of contact regarding all contractual matters, including payment of any and all charges resulting from any Contract.

5. Related Documents Required

The selected Vendor will be required to submit the following documents prior to Contract approval:

a) Certificate of Good Standing obtained by the Secretary of State of New Hampshire.

b) Certificate of Authority/Vote - The Certificate of Authority/Vote authorizes, by position, a representative(s) of your corporation to enter into an Agreement or amendment with the State of New Hampshire.

c) Certificate of Insurance - Certificate of Insurance evidencing coverage as required under the Contract.

d) Workers' Compensation coverage must comply with State of NH RSA 281-A.

Remainder of this page intentionally left blank.

APPENDIX A: VENDOR CONFERENCE REQUIREMENTS

Applicable
An Optional Vendor Conference will be virtually held on the date and at the time identified in the Schedule of Events.

All Vendors who intend to submit Proposals are encouraged to attend the Vendor Conference.

The meeting link and access instructions will be emailed to registrants upon request. Vendors are requested to RSVP via email by the date identified in the Schedule of Events, indicating the number of individuals who will attend the Vendor Conference.

Vendors are allowed to send a maximum number of three (3).

Vendors will have an opportunity to ask questions about the RFP and the State will make a reasonable attempt to answer questions it deems appropriate. Questions may include, without limitation, a request for clarification of the RFP; a request for changes to the RFP; suggestions or changes to the RFP that could improve the RFP competition or lower the offered price; and to review any applicable Documentation.

Vendors are encouraged to email two days before the Vendor Conference. No responses will be given prior to the Vendor Conference. Oral answers will not be binding on the State. The State's final response to Vendor inquiries and any requested changes to terms and conditions raised during the Vendor Inquiry Period will be posted to the DAS Website by the date specified as the final State responses to Vendor inquiries as specified in the Schedule of Events. Vendors are responsible for any costs associated with attending the Vendor Conference.

Remainder of this page intentionally left blank.

APPENDIX B: BUSINESS/TECHNICAL REQUIREMENTS AND DELIVERABLES

1. Statement of Work

The Contractor shall furnish all labor, project management, professional services, software development and/or configuration, infrastructure and hosting services where applicable, integration services, documentation, testing, training, deployment, transition, maintenance, and support necessary to deliver a complete and operational solution that modernizes the public-facing Sex Offender Registry website and related administrative capabilities.

The State does not prescribe a specific software, development, hosting, or deployment model for the Solution. The proposed Solution may be provided as a custom-developed, Commercial Off-the-Shelf (COTS), Software-as-a-Service (SaaS), Vendor-hosted, State-hosted, cloud-hosted, or hybrid solution, provided that the proposed Solution meets the requirements of this RFP. The Vendor shall identify the proposed Solution architecture and hosting/deployment model and clearly identify the responsibilities of the State and Vendor for infrastructure, hosting, software, security, maintenance, support, backup, disaster recovery, and system administration.

The awarded solution shall improve the State's ability to publish approved registry information to include non-compliant offender warrant list, administer annual fee payment activity, manage operational records, reporting, audit history, and exception processing, and support long-term maintainability within the State's technical and business environment as well as provide reciprocity with other jurisdictions.

2. Business and Technical Requirements

Please utilize the following instructions to complete all tables under 2.1 Business Requirements and 2.2 Technical Requirements and submit with your Proposal in Section III: Responses to System Requirements and Deliverables.

Remainder of this page intentionally left blank.

Criticality Column:

(M) Indicates a requirement that is "Mandatory." The State considers it to be of such great importance that it must be met for the Proposal to be accepted. If the proposer believes that there is something about their Proposal that either obviates the need for this requirement or makes it of less importance this must be explained within the comments. The State retains the right to accept a Proposal if the need of the requirement is reduced or eliminated by another feature of the Proposal.

(P) Indicates a requirement which is "Preferred." This requirement is considered by the State to be of great usefulness, but the lack of this feature is not considered serious enough to disqualify the Proposal.

(O) Indicates a requirement which is "Optional." This requirement is considered by the State to be one which is useful or potentially useful but not a central feature of the Project.

Vendor Response Column:

Enter “Yes” if the Solution can fully support ALL the functionality described in the row, without special customization. “Yes” can only be used if the delivery method is Standard (see delivery method instructions below).

Otherwise, enter "No"; "No" can only be used with delivery method Future, Custom, or Not Available/Not Proposing (see delivery method instructions below).

Vendor Delivery Method Column:

Complete the delivery method using Standard, Future, Custom, or Not Available/Not Proposing (as defined below) that indicates how the requirement will be delivered.
Standard – Feature/Function is included in the proposed Solution and available in the current Solution release.

Future – Feature/Function will be available in a future release. (Provide anticipated delivery date, version, and service release in the comment area.)

Custom – Feature/Function can be provided with custom modifications. (Respondent must provide estimated hours and average billing rate or flat cost for the modification in the comment area. These cost estimates should add up to the total cost for modifications found in the cost summary table in Appendix E of the RFP).

Not Available/Not Proposing – Feature/Function has not been proposed by the Vendor. (Provide brief description of why this functionality was not proposed.)

Vendor Comments Column:

For all Delivery Method responses, vendors must provide a brief explanation of how the requirement will be met. Free form text can be entered into this column.

2.1. Business Requirements

Table B-2.1 Business Requirements

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
B1.1	The solution shall provide a modern public-facing Sex Offender Registry website that publishes only State-approved public registry information from the authoritative source of record.	M			
B1.2	The public website shall allow search by offender name, address, municipality, zip code, and configurable radius from a validated location.	M			
B1.3	The public website shall provide map-based search and display, including address geocoding and configurable radius search.	M			
B1.4	The public website shall be mobile responsive and accessible in conformance with WCAG 2.1 AA or State-approved successor standard.	M			
B1.5	The public website shall support a configurable FAQ / informational content section maintained by authorized State staff.	M			
B1.6	The solution shall support payment by card and shall also support the administrative ability to accept and record cash or check transactions when permitted by State process.	M			
B1.7	The existing State registry shall remain the authoritative system of record unless the State expressly designates otherwise in the resulting contract.	M			
B1.8	The solution shall support at least daily synchronization of approved public data from the authoritative registry source to the public website.	M			
B1.9	The solution shall log, track, and report data synchronization failures, publication failures, and retry outcomes.	M			

B1.10	The solution shall support public tip or comment submission with configurable routing, spam prevention, and required public disclaimers.	M			
B1.11	The solution shall support configurable public display rules, including suppression, disclaimer text, and content governance controls.	M			
B1.12	The solution shall provide role-based administrative access with permissions aligned to user job functions.	M			
B1.13	The solution shall maintain complete audit history for user access, administrative actions, publication events, etc.	M			
B1.14	The solution shall support structured reporting and export capability for publication activity, exception queues, audit history, and operational metrics.	M			
B1.15	The solution shall preserve change history for material data elements and support-controlled correction workflows.	M			
B1.16	The solution shall support integration with the existing registry environment which will be maintained as the system of record.	M			
B1.17	The solution shall provide configurable notices, labels, and workflow states sufficient to distinguish draft, pending, finalized, voided, corrected, and superseded transactions.	M			
B1.18	The solution shall support production AND test environments and shall include migration / promotion controls between environments.	M			
B1.19	The solution shall support configurable business rules so that changes to policy, workflow, display rules, or operational handling can be implemented without full system redesign where practicable.	M			

B1.20	The solution shall integrate with the State's Payment Adapter provided by CyberSource for collection of annual fees as outlined in RSA 651-B:11	M			
B1.21	The solution shall support a warrant list workflow for non-compliant offenders and ensure public publication strictly matches RSA 651-B:7 rules. Law-enforcement-only fields shall be segregated and not published on the public site; the solution shall support internal access for authorized personnel and appropriate audit/logging	M			
B1.22	The proposed Solution may be provided using a custom-developed, Commercial Off-the-Shelf (COTS), Software-as-a-Service (SaaS), Vendor-hosted, State-hosted, cloud-hosted, or hybrid deployment model, provided that the proposed Solution satisfies all applicable requirements of this RFP. The Vendor shall identify the proposed hosting and deployment model and clearly identify the responsibilities of the State and Vendor for infrastructure, hosting, software, security, maintenance, support, backup, disaster recovery, system administration, and other operational responsibilities associated with the proposed Solution.	M			
B1.23	The solution shall provide Single Sign-On (SSO) for all internal users (administrators and staff) to access and perform administrative (back-end) functions across non-public interfaces.	M			

2.2.

2.3. Technical Requirements

Table B-2.2.1 Prohibited Technologies

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
PT1	No equipment or services on the State of New Hampshire's Prohibited Technologies List found here: Prohibited Technologies List and No equipment or services on the FCC Covered List found here: FCC Section 2 List of Equipment and Services	M			

Table B-2.2.2 Security Compliance Requirements

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
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. 3, 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			

Remainder of this page intentionally left blank.

Table B-2.2.3 GovRAMP Authorization

Applicability: The requirements in this section relating to GovRAMP, FedRAMP, and other cloud security authorizations apply to Vendor-hosted, cloud-hosted, SaaS, PaaS, IaaS, or other externally hosted components of the proposed Solution, as applicable. These requirements shall not apply to components deployed entirely within State-controlled infrastructure. Vendors shall identify the components of their proposed Solution to which these requirements apply.

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
T2.1	**Vendor-Hosted Solutions:** If the proposed Solution is Vendor-hosted, the Vendor shall identify the hosting/service model and provide the current security authorization, certification, assessment, or other independent security assurance applicable to the proposed Solution and hosting environment.	M			
T2.2	**Vendor-Hosted Solutions:** If the proposed Solution is GovRAMP Authorized, GovRAMP Ready, or otherwise participating in the GovRAMP Security Program, the Vendor shall identify its current status and provide supporting information sufficient for the State to verify that status.	P			
T2.3	**Vendor-Hosted Solutions:** If the proposed Solution is not GovRAMP Authorized, the Vendor shall describe its current security posture, applicable independent security assessments or certifications, and its planned approach to meeting all applicable State security requirements.	M			
T2.4	**State-Hosted/On-Premises Solutions:** GovRAMP authorization is not applicable. The Vendor shall instead provide documentation describing how the proposed Solution will comply with applicable State security requirements, including the applicable security architecture, access controls, vulnerability management, patch management, logging and monitoring, data protection, security testing, incident response, backup and recovery, and other applicable controls.	M			
T2.5	The Vendor shall identify any material security dependencies on third-party products, services, hosting providers, infrastructure, or other technologies required for the proposed Solution and describe how those dependencies will be secured and monitored.	M			

T2.6	For any resulting Contract, the Vendor shall provide the State with reasonable access to applicable security documentation, assessments, audit reports, vulnerability assessments, penetration testing results, and other evidence necessary to evaluate ongoing compliance with the Contract's security requirements, subject to applicable confidentiality and security restrictions.	M			

Table B-2.2.4 Security Certifications and Independent Assessments

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
T3.1	FedRAMP Authorized https://www.fedramp.gov/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			
T3.3	SOC 2 Type II or comparable independent security audit	P			

Table B-2.2.5 Vendor-Hosted Platform

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
T4.1	The following Hosting Platforms are FedRAMP/GovRAMP 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			

Table B-2.2.7 Information Technology Accessibility Compliance

Req #	State Requirement Description	Criticality	Vendor Response	Vendor Delivery Method	Vendor Comments
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 ITI Accessibility Policy	M			

2.4. Service Level Agreement (SLA)

Vendor agrees to the following Service Level Requirements

Req #	State Requirement Description	Criticality
SLA -1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M
SLA -2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing upgrades and fixes as required.	M
SLA -3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M
SLA -4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers. (RA-5)	M
SLA -5	The State shall have unlimited access, via phone or email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M

SLA -6	The Vendor shall conform to the specific deficiency class as described below or as agreed to by the parties: • Class A Deficiency – Software – Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation – missing significant portions of information or unintelligible to State; Non-Software – Services were inadequate and require re-performance of the Service. • Class B Deficiency – Software – important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation – portions of information are missing but not enough to make the document unintelligible; Non-Software – Services were deficient, require reworking, but do not require re-performance of the Service. Class C Deficiency – Software – minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation – minimal changes required and of minor editing nature; Non-Software – Services require only minor reworking and do not require re-performance of the Service.	M
SLA -7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: Class A Deficiency – The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; Class B & C Deficiency – The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.	M
SLA -8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M
SLA -9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M
SLA -10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M
SLA -11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M
SLA -12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M

SLA -13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M
SLA -14	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M
SLA -15	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M
SLA -16	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1. Nature of the Deficiency. 2. Status of the Deficiency. 3. Action plans, dates, and times. 4. Expected and actual completion time. 5. Deficiency resolution information. 6. Resolved by. 7. Identifying number i.e., work order number. Issue identified by.	P
SLA -17	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1. Mean time between reported Deficiencies with the Software. 2. Diagnosis of the root cause of the problem. Identification of repeat calls or repeat Software problems.	P

3. Activity, Deliverable, or Milestone

Vendor shall be responsible for meeting the Deliverables, Activities and/or Milestones identified in Table B-3: Deliverables.

Table B-3: DELIVERABLES

PLANNING AND PROJECT MANAGEMENT

1	Project Kickoff Meeting and Kickoff Materials	Non-Software
2	Detailed Work Plan, Schedule, Deliverables, Dependencies, and Payment Milestones	Written
3	Project Status Reports and Risk / Issue Log	Written
4	Infrastructure Plan, including Desktop, Network, Environment, Hosting, and Configuration Requirements	Written
5	Security Plan and Access Control Design	Written
6	Communications and Change Management Plan	Written
7	Software Configuration and Release / Promotion Plan	Written

8	Systems Interface Plan and Design / Capability	Written
9	Testing Strategy, Master Test Plan, Scripts, Results, and Defect Management Support	Written
10	Data Conversion / Migration Plan and Design	Written
11	Deployment / Cutover / Go-Live Plan	Written
12	Comprehensive Training Plan, Curriculum, and Training Materials	Written
13	End User Support Plan	Written
14	Business Continuity and Disaster Recovery Plan	Written
15	Documentation of Operational Procedures, Administrator Guide, and Operations Support Guide	Written

INSTALLATION

16	Business Process Validation Document	Written
17	Requirements Traceability Matrix	Written
18	Solution Design Document	Written

TESTING

19	Data Dictionary and Field Mapping Document	Written
20	Payment Workflow and Reconciliation Design	Written
21	Role and Permission Matrix	Written
22	Exception Handling and Manual Workaround Procedures	Written
23	Production Readiness Checklist	Written
24	Final Configuration / As-Built Documentation	Written

SYSTEM DEPLOYMENT

25	Post-Go-Live Support Plan	Written
26	Project Closeout / Exit Meeting and Final Project Summary	Non-Software

PROJECT COMPLETION

27	Conduct Project Exit Meeting	Non-Software

4. Data Location

The Vendor shall provide its Services to the State and its end users solely from data centers within the Continental United States. All storage, processing and transmission of State Data shall be restricted to information technology systems within the Continental United States. The Vendor shall not allow its personnel or sub-contractors to store State data on portable devices, including personal computers, except as specified and allowed by the Contract, and then only on devices that are used and kept at its data centers within the Continental United States. The Vendor shall permit its personnel and contractors to access State data remotely only to provide technical support and as specified or required by the Contract.

5. Background Checks

The Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the State's information among the Contractor's employees and agents.

The State may, at its sole expense, conduct reference and background screening of the Contractor's Project Manager and Key Project Staff. The State shall maintain the confidentiality of background screening results in accordance with the Contract Agreement.

Remainder of this page intentionally left blank.

APPENDIX C: TOPICS FOR MANDATORY RESPONSES

This section provides a series of technical topics that the State of New Hampshire will consider in selecting a Solution for this RFP. Responses provided should be relevant to the Project described within this RFP. Vendors must limit narrative responses describing the Software, Technical, Services and Project Management topics defined for this Project. The following table identifies specific topics for narratives. A page limit is identified for each topic. If a response to a topic exceeds the page limit, the State will limit its consideration to the prescribed page limit.

Table C: Topics

1. Proposed Solution

TOPIC	PAGE LIMIT
Topic 1 – Description of Solution	7 - Attachment Unlimited (optional)
Topic 2 – Technical Architecture	5
Topic 3 – Software Releases	5

2. Vendor's Technical, Service and Project Management Experience

2.1. Security and Protection of Data

TOPIC	PAGE LIMIT
Topic 4 – System Security	10
Topic 5 – Security Testing	3

2.2. State Personnel and Training

TOPIC	PAGE LIMIT
Topic 6 – User Training Approach	3
Topic 7 – Preparation and Expectations of State Staff including Technical Knowledge Transfer	4

2.3. Project Execution

TOPIC	PAGE LIMIT
Topic 8 – Implementation Approach	10
Topic 9 – Testing Management	6
Topic 10 – Migration Strategy	3
Topic 11 – Environment Setup	2

2.4. Project Management

TOPIC	PAGE LIMIT
Topic 12– System Acceptance Criteria	6
Topic 13 – Work Plan, Status Meetings and Reports	No Limit
Topic 14 – Risk and Issue Management	3
Topic 15 – Scope Control	2
Topic 16 – Quality Assurance Approach	6

2.5. Ongoing Operations For Vendor Hosted Solution

TOPIC	PAGE LIMIT
Topic 17 – Hosted System	5
Topic 18 – Backup and Recovery	2
Topic 19 – Assurance and Business Continuity Plan	3
Topic 20 – Support and Maintenance for Vendor Hosted System	2

2.6. Ongoing Operations For State Hosted Solution

TOPIC	PAGE LIMIT
Topic 21 – Support and Maintenance for State Hosted System	2

1. Proposed Solution

TOPIC 1 - DESCRIPTION OF SOLUTION

The State will evaluate whether the proposed Solution includes the required features.

1) Provide a detailed description of your proposed Solution, including features and functionality.
2) Describe how your Solution meets the business requirements in B-2 Business Requirements/Technical Requirements.
3) Identify the proposed Solution model, including whether the Solution is custom-developed, COTS, SaaS, Vendor-hosted, State-hosted, cloud-hosted, or a hybrid of these models. Describe the rationale for the proposed model and identify any significant dependencies, assumptions, or limitations associated with the proposed approach.
4) Describe ease of use and user friendliness of your proposed Solution including learning curve, navigation. Highlight in detail specific advantages to the user Interface. What methodology do you use to ensure that your user Interface is user friendly?
5) Provide an attachment with product literature describing the functionality of the proposed Solution. Provide a table that maps your literature with topics listed in this Appendix. Include references to page numbers.
6) Describe how an offender would pay their registration fee online through the credit card processing application?
7) Describe the mapping public user interface?

TOPIC 2 - TECHNICAL ARCHITECTURE

The State will evaluate the degree to which the architecture can be supported over an extended period, including the ease of support.

1) Describe the technical architecture (software, hardware, and Network) of the proposed Solution.
2) Describe how your Solution meets the technical requirements in B-2 Business Requirements/Technical Requirements.
3) Describe the benefits of the technical architecture (i.e. scalability, adaptability, interoperability, etc.)
4) How will the proposed Solution be accessed (i.e. Web Browser over Internet)?
5) Describe any additional software that will be required on end-point devices and the access authorization level required to install it.
6) Describe any add-on or third-party Software required.
7) Is your product dependent on a solution not included in this Proposal?
8) What programming languages are used for development, configuration, and customization of the proposed Solution? When was the core Software written?
9) What components of the Software, such as Middleware, are proprietary?
10) Is the proposed application considered Open-Source Software?
11) Describe any Open-Source Software used by the proposed Solution.
12) Describe the degree to which the proposed Solution meets the requirements of RSA chapter 21-R:10, 21-R:11, 21-R:13, 21-R:14. Chapter 21-R DEPARTMENT OF INFORMATION TECHNOLOGY (state.nh.us)
13) Describe any hardware requirements associated with the hardware Solution.
14) Describe the proposed hosting and deployment architecture, including which components will be hosted or managed by the Vendor and which components, if any, will be hosted or managed by the State. Identify all infrastructure, software, database, middleware, network, security, licensing, third-party service, and other technical dependencies required to operate the proposed Solution.

TOPIC 3 - ENHANCEMENTS AND NEW RELEASES

The State will evaluate the degree to which the solution appears likely to evolve and the burden, if any, of keeping pace with the expected evolution.

Discuss the following aspects of anticipated future releases of the proposed Solution. Coverage should include but not be limited to the following:

1) What types (maintenance, Enhancement, other) of releases are planned?
2) What is the historical (past 3 years) and expected frequency of each type of new release?
3) How is the content of future releases determined? Required maintenance, security, user input?
4) Are Enhancements made for specific clients included in future releases for all clients?
5) What specific Enhancements are planned for release within the next 24 months?
6) How is the content of a release communicated to the client?
7) Can components of a release be applied individually or by Module without adversely affecting the overall functionality of the System?
8) How long is a release supported?

2. Vendor's Technical, Service and Project Management Experience

(Vendors whose product has a status of GovRAMP Ready or Authorized do not complete C-2.1, go directly to C-2.2 State Personnel and Training)

2.1. Security and Protection of Data

TOPIC 4 - SYSTEM SECURITY

The State will evaluate the degree to which the proposed System is designed and architected to ensure the confidentiality and integrity of its valued asset, Data.

Describe the System security design and architectural features incorporated into the proposed Solution including:

1) Compliance with NIST SP 800-171, Protecting Controlled, Unclassified Information in Non-Federal Systems and Organizations.
2) Compliance with NIST SP 800-63, Digital Identity Guidelines.
3) Compliance with NIST SP 800-115, Technical Guide to Security Testing and Assessment.
4) The methods used to ensure that the parties to interactions with the Application cannot later repudiate or rebut those interactions.
5) The Intrusion Detection methods used to ensure the detection, recording and review of attempted access or modification by unauthorized individuals.
6) The privacy methods used to ensure that Confidential Data and sensitive communications are kept private.

7) The system maintenance methods used to ensure that system maintenance does not unintentionally disrupt the security mechanisms of the Application or supporting hardware.

8) Your Software patch schedule employed to protect the Software from new security vulnerabilities as they arise.

9) The ability of your Software to be installed in a "locked-down" fashion to turn off unnecessary features (user accounts, Operating System Services, etc.) thereby reducing the Software's security vulnerabilities and attack surfaces available to System hackers and attackers.

10) The notification and escalation process in the event of an intrusion.

11) Describe the System assurance provisions incorporated into the proposed Software. At a minimum, discuss the following:

    a) What process or methodology is employed within the proposed Software to ensure Data integrity?

    b) To what degree does your approach rely on System assurance capabilities?

    c) If multiple Databases are employed, what extra procedures are employed to ensure synchronization among Databases?

TOPIC 5 - SECURITY TESTING

The State will evaluate the Vendor's approach to Security Testing.

1) Describe the testing tools and methodologies used for testing the security of the Software Application and Hosting environment.

2) How can you ensure the security and confidentiality of the State Data collected on the system?

3) What security validation Documentation will be shared with the State?

4) Do you use internal or external resources to conduct Security Testing?

Remainder of this page intentionally left blank.

2.2. State Personnel and Training

TOPIC 6 - USER TRAINING APPROACH

The State will evaluate whether the training approach is likely to prepare users adequately to use the new System from the day of deployment, including maximum knowledge transfer to allow the State to conduct its own training in the future.

1) Describe in detail the options for Vendor-supplied training. Include a proposed training schedule, training topics, and options for participation (e.g., in-person, webinars, one-on-one, online on-demand) that you would provide.
2) Describe in detail the Documentation that is available to support the training of users of your proposed Solution. Include help screens, online or printable manuals and Knowledge bases. If any of these resources would need to be developed or modified for your proposed Solution include a timeline for their availability. If there are access restrictions on any of this material indicate what those restrictions are.

TOPIC 7 - PREPARATION AND EXPECTATIONS OF STATE STAFF INCLUDING TECHNICAL KNOWLEDGE TRANSFER

The State will evaluate whether the provisions to prepare State staff participating in the Project will enable the staff to contribute appropriately and the State will evaluate requirements for State staff to support the system after Implementation.

1) Describe how State staff assigned to the Project Team will be involved throughout the Project, including design meetings, decision making, and scope control.
2) Provide an overview of Project Team interactions and dependencies between functions.
3) Provide recommendations for State staff requirements to maintain the system after Implementation (skill, # of resources, etc.). Include a worksheet or table identifying State staff resources and the projected number of weekly hours to support the system moving forward.
4) The transfer of technical knowledge is important for operations, configuration/development, workflow, business setup, maintenance, and management. Address, training curriculum, training priorities and prerequisites, specific commercial and custom course, and one-on-one learning opportunities for State staff.
5) Describe and provide samples of the available Documentation supporting the System. Does the Documentation include technical specifications, troubleshooting tips, technical contact information?
6) Please utilize Table C-2.2 Proposed State Staff Resource Hours to indicate the State roles that will need to be assigned to the Project to support your proposed Implementation approach. Information is required by stages identified in the table below.

Table C-2.2 Proposed State Staff Resource Hours

State Role	Planning and Project Management	Installation and Testing	System Deployment	Ongoing Operations	Total Hours
Project Manager					
Position #1					
Position #2					
Position #3					
TOTALS					

NOTE to Vendor: Key Assumption(s): Denote key roles by adding "(key)" to the 'State Role' column. Add as many rows as necessary to complete the full proposed team.

2.3. Project Execution

TOPIC 8 - IMPLEMENTATION APPROACH

The State will evaluate the quality of analysis, reasonableness, and flexibility evident in the proposed Implementation approach.

1) Provide one or more feasible Implementation Plans. For each plan provided:
   a) Identify timeframes for major milestones, including timing for discontinuing legacy Systems.
   b) Discuss cost implications of the plan, including implications on maintenance fees and available Implementation options that would lower prices.
   c) Address the level of risk associated with each plan.
   d) Discuss why this is the approach you recommend?
2) Will the Vendor provide a tool for the State and the Vendor to communicate and share information throughout the Project – i.e., SharePoint, Portal?

TOPIC 9 - TESTING MANAGEMENT

The Contractor shall provide end-to-end planning and preparation for testing and Acceptance of solutions throughout the Project using an industry standard methodology. This shall include training, a detailed testing methodology which covers all "areas of testing," security, required staffing with clear roles and responsibilities, test cases and scripting with associated Data, status and results Reporting. The Test Plan defined shall ensure designed and implemented Solutions are fully supported, tested, and documented.

It is anticipated that the test phases in Table C-2 Testing will be included in the Project described in this RFP. The State will evaluate the quality of testing approach used by the Vendor.

1) Describe in detail the end-to-end testing methodology you propose for this Project.
2) Describe testing tools that will be used as part of the Solution testing. Will these tools be available to the State or will the State be required to purchase tools?
3) Using the following chart, describe the roles and responsibilities required of Vendor Staff and State Staff, include additional information as needed.

Test Phase	Vendor Role /Responsibility	State Role /Responsibility	Tools	Time-frame
Management of the Testing Process				
Test planning				
Test scenario development				
Data preparation				
System preparation				
Unit Testing				
System integration testing				
Defect tracking				
Application stress testing and tuning.				

4) What support will be provided to prepare State staff prior to and during Acceptance Testing? (Training, user Documentation, staff on site, remote support, etc.)
5) Will configured Software be delivered in functional components for State Acceptance Testing?
6) The State has defined 3 levels of Defect severity. Describe how you will adopt this methodology or provide a mapping to outline your proposed representation of Defect severity.
7) What tools will be used to document and track status of suspected Defects?
8) What role will the State play in classification and prioritization of Defects?
9) How quickly will a suspected Defect be investigated and how quickly will the Defects be corrected?
10) Provide a sample User Acceptance Test Plan from a completed project as an appendix.
11) Will System performance be measured and documented using the State's infrastructure and Data? If yes, how? (Not needed for Hosting?)
12) Outline your methodology for Security and Penetration Testing and provide confirmation that it is NIST SP800-115 compliant.

Remainder of this page intentionally left blank.

TOPIC 10 - MIGRATION STRATEGY

The State will evaluate the degree to which the Vendor will ensure that Data conversion is effective and impacts State staff to the minimum extent possible.

It is our assumption that the Data Conversion/Migration Plan is a Deliverable that will ultimately lay out the plan required to convert and migrate Data from the State's existing Sex Offender Registry system legacy system to the new environment. Discuss your high-level approach to carrying out Data conversion/migration activities. Be sure to discuss software tools and processes used to support this effort.

1) Describe the approach that will be used for assessing Data quality and conducting Data cleansing prior to conversion. Be sure to include whose responsibility it will be and the process you are proposing to deal with incomplete records in the legacy system.
2) Discuss the use of automated tools in Data conversion. When will automated tools be used? When will manual intervention be required?
3) What Data do you know will be challenging to convert/migrate and why? What special approach will you recommend as part of the planning document to help reduce the impact of this challenge on this Project?
4) Discuss your approach to working with the Agency to document a Data conversion/migration plan and process. Describe how you will determine how much historical Data is available and what is appropriate to be made available within the new system.
5) Define expectations for State and Vendor roles during the development of the Data conversion/migration plan and process.
6) What lessons learned can you share with us from other Implementations that are important to understand as part of development of the Data conversion/migration plan and process?

TOPIC 11 - ENVIRONMENT SETUP

The State will evaluate whether proposed environments are sufficient to satisfy Project needs, including phased Implementation.

1) Describe the different Software and hardware environments required for the concurrent development, testing, and production of the proposed Solution. Discuss how the proposed environments support the implementation of the solution, including all necessary training.
2) The State believes that additional Software License fees solely related to establishing environments for normal development lifecycle would be inappropriate. If the Proposal differs from this standard, describe and provide rationale for the difference.
3) Provide diagrams of the environment including Data architecture, Data flows (Include as an attachment).
4) Describe the ramifications to the State if the recommended environment is not followed (example – separate Database and Application Server works better for clients).

2.4. Project Management

TOPIC 12 - SYSTEM ACCEPTANCE CRITERIA

The State will evaluate whether proposed Acceptance criteria will assure the State that the new System is functioning effectively before being turned over for State for User Acceptance Testing.

1) Propose measurable criteria for State final Acceptance of the System.
2) Discuss how the proposed criteria serve the interest of the State.

TOPIC 13 - WORK PLAN, STATUS MEETINGS AND REPORTS

The State will evaluate whether the Vendor's preliminary proposed Work Plan includes a description of the Schedule, tasks, Deliverables, major milestones, task dependencies, and a payment Schedule. The Work Plan shall also address resource allocations (both State and Vendor team members). This narrative should reflect current Project Management "best practices" and be consistent with narratives on other topics. The Software to be used to support the ongoing management of the Project should also be described in the Work Plan. Additionally, the State will evaluate the degree to which Project Reporting will serve the needs of State Project leaders.

The State sees a Work Plan as essential to reaching a comprehensive agreement with a Vendor. Consequently, the State will seek to refine the proposed Work Plan prior to Contract approval with the selected Vendor and to incorporate the refined Work Plan by reference into a Contract.

1) Provide a preliminary Work Plan depicting tasks, task dependencies, Schedule, milestones/critical events, Deliverables, and payment Schedule. Include the Deliverables outlined in Appendix B (Business/Technical Requirements and Deliverables), appropriate status meetings and Reports, and include other Deliverables that you, based on experience, would recommend be developed on this Project.
2) Define both proposed Written and Software Deliverables. Include sufficient detail that the State will be able to identify departures from the Plan in sufficient time to seek corrective action. Provide information about staffing.
3) Describe all Deliverables to be produced in the Project. Ensure that all Deliverables and milestones are identified in the Work Plan. Identify and discuss the following:

a) All assumptions upon which the Work Plan is based.

4) Descriptions of recommended roles by activity and time required for both State and Vendor members of the Project Team.
5) Assignments of members of the Vendor's team identified by role to specific tasks.
    a) Critical success factors for the Project.
6) Discuss how this Work Plan will be used and State access to Plan details.
7) Discuss frequency for updating the Plan, at a minimum biweekly and for every status meeting. Explain how the State will know whether the project is on schedule, project expenses incurred to date, and within budget.

8) Define your planned approach to maintaining all project documentation. For example, how will this documentation be available to the State staff (Word Doc, SharePoint, etc.).

9) Describe your approach to knowledge transfer between all Vendor project teams for completion of all deliverables defined in this RFP and resulting contract.

   The State will evaluate the degree to which Project Reporting will serve the needs of State Project leaders.

10) The State believes that effective communication and Reporting are essential to project success. As reasonably requested by the State, Vendor shall provide the State with information or reports regarding the Project. Vendor shall prepare special reports and presentations relating to Project Management and shall assist the State in preparing reports and presentations, as reasonably requested by the State, all at no additional price to the State.

11) Describe your planned project management activities including Introductory and Kickoff Meetings, Status Meetings, Work Plan Updates, and Special Meetings. Discuss frequency, duration, participants, agenda items, etc.

12) Describe how you will report Project health to communicate Project status with Stakeholders and for the early recognition of factors that may result in Project problems requiring special attention.

TOPIC 14 - PROJECT RISK AND ISSUE MANAGEMENT

The State will evaluate the extent to which the proposed approach will contribute to the timely identification and effective action on project issues and risks. The State will also evaluate whether the approach recognizes and addresses appropriate State involvement in project risk and issue management.

1) Provide proposed methodologies for project risk and issue management. Discuss State and Vendor responsibilities. The State seeks a clear means to compare planned versus actual status, including percentages, at a sufficiently detailed level to ensure the State can adequately monitor the progress of the Project. Be sure to identify any essential time constraints on State actions. Escalation procedures will be defined in a Contract between the State and the Vendor.

Remainder of this page intentionally left blank.

TOPIC 15 - SCOPE CONTROL

The State will evaluate the degree to which proposed modifications in scope are scrutinized to ensure that only essential changes are approved. Evaluation will also address the quality and timeliness of information that will be available about a proposed scope change.

1) Demonstrate your firm's ability to manage scope creep by discussing tools and methodologies, as well as past project experiences.

TOPIC 16 - QUALITY ASSURANCE APPROACH

The State will evaluate the degree to which proposed procedures will ensure that Deliverables require limited modification when submitted for approval.

1) Describe the methodology that will be employed to assure that each type of Deliverable is of high quality before submission for State consideration (Written, Software, and Non-Software). Discussion should include but not be limited to:
   a) Provision for State input to the general content of a Written Deliverable and Non-Software Deliverables prior to production.
   b) The standard for Vendor internal Review of a Written Deliverable and Non-Software Deliverables prior to formal submission.
   c) Testing of Software Deliverables prior to submission for Acceptance Testing.

2.5. Ongoing Operations for Vendor Hosted Solution

(Vendors whose product has a status of FedRamp or GovRAMP Ready or Authorized do not complete 2.5.)

TOPIC 17 -HOSTING AND SECURITY ARCHITECTURE

1) Describe the service model being offered. Service is Commercial Off-the-Shelf Software (COTS), Software-as-a-Service (SaaS), Platform-as-a-service (PaaS), or Infrastructure-as-a-Services (IaaS). Refer to the glossary for definitions.
2) The State requires the service provider to use web services exclusively to Interface with the State of New Hampshire's Data in near Real-Time when possible. Describe any client software or plug-in downloads that may be required.

   It is preferred the service provider's relevant Data Center(s) are certified to the Federal Information Security Management Act (FISMA) level 3 ATO4 and/or Federal Risk and Authorization Management Program (FedRAMP) CSP5, and have independent annual SOC 2 Type 2 audits performed.
3) Provide Certifications and latest audit of the Data Center(s) being used in the Solution offered.

4) If Certifications and audits cannot be provided the service provider will be required to implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Information and Non-Public Information. Such security measures must be in accordance with recognized industry practices such as in the National Institute of Standards and Technology (NIST) Controls 800-53 Rev 4 where applicable. Describe controls including but not limited to:
    a) data storage, data encryption, data destruction, data location, and data handling.
    b) business continuity and disaster recovery plan.
    c) security incident or data breach notification.
    d) change control.
    e) maintenance, patching and upgrades.
5) Describe how the service provider will provide compliance to all Federal and State of New Hampshire laws, regulations, statutes, policies, standards, and best practices relevant to internet-based Hosting.
6) The State requests regularly scheduled Reporting to the State of New Hampshire. Describe the availability of Reports available to the State including latency statistics, user access, user access IP address, user access history and security logs for all State of New Hampshire files related to this RFP.
7) The State requires the system to be available 24/7/365 (with agreed-upon maintenance downtime), and for the Vendor to provide service to customers as defined in a Service Level Agreement (SLA) which will be developed and agreed to in the Contract phase. The State also requires the service provider to guarantee 99.9% uptime (excluding agreed-upon maintenance downtime). Describe how you will meet these requirements.

TOPIC 18 - BACKUP AND RECOVERY

The State seeks a sound Backup and Recovery provision as part of the Solution.

1) Describe the tools used for Backup and Recovery of Applications and Data.
2) Describe timelines for scheduled backup of Data and Servers including the retention schedule.
3) Describe the impact of the proposed backup process on the operation of the System. Also, address the following:
    a) Use of and method for logging and journaling.
    b) Single points of failure and recommended approaches for their elimination.
    c) Approach to redundancy including backup material securely transferred from the site to another secure location to avoid complete Data loss with the loss of a facility.
4) Explain your high-level methodology for creation of a Disaster Recovery Plan.

5) Discuss how the disaster recovery plan identifies appropriate methods for procuring additional hardware in the event of a component failure. Also describe any impact of Software License fees. The State believes that additional Software License fees solely related to redundancy for Backup and Recovery would be inappropriate. If the Proposal differs from this standard, describe and provide rationale for the difference.

6) Discuss how the disaster recovery plan addresses the recovery of lost State Data as well as your own.

7) Will the Solution include the option to have the collected Data stored at the Vendor's site, at the State site or both?

TOPIC 19 - ASSURANCE OF BUSINESS CONTINUITY

The State will evaluate the degree to which the proposed plan to assure business continuity mitigates risk to the State, and its potential for Implementation (cost effective and easy to implement).

1) Provide a plan for business continuity if a disaster occurs at the Data center that is Hosting the proposed Solution.

2) The State believes that additional Software License fees solely related to redundancy for assurance of business continuity would be inappropriate. If the Proposal differs from this standard, describe and provide rationale for the difference.

TOPIC 20 - SUPPORT AND MAINTENANCE FOR VENDOR HOSTED SYSTEM

The State will evaluate whether the Vendor's proposed support and maintenance plan includes a description of the types and frequency of support, detailed maintenance tasks – including Scheduled maintenance and upgrades, and any other dependencies for on-going support and maintenance of the system. This narrative should reflect current "best practices" for these tasks.

1) Describe how the System hardware, Software, and Database will be maintained in accordance with the Specifications, terms, and conditions of the RFP, including providing upgrades and fixes as required.

2) Describe the Help Desk Support that will be available to State staff including hours of operation, phone vs email, access to technical support staff.

3) Describe the classification of a Software Defect (bug) that will be used to indicate the degree of negative impact on the quality of the Software and anticipated response times.

4) Describe any procedures required to handle escalation and emergency calls.

5) Detail the types and frequency of support tasks required.

6) Describe any different levels and or models of support and maintenance that you provide.

7) Describe how the Vendor will work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information:
   a) mean time between Reported Deficiencies with the Software.
   b) diagnosis of the root cause of the problem.
   c) identification of repeat calls or repeat Software problems.
8) For all maintenance service calls, the Vendor shall ensure the following information will be collected and maintained:
   a) Nature of the Deficiency.
   b) Status of the Deficiency.
   c) Action plans, dates, and times.
   d) Expected and actual completion time.
   e) Deficiency resolution information.
   f) Resolved by.
   g) Identifying number i.e. work order number.
   h) Issue identified by.
9) Describe how the State will be informed of emergency maintenance or system outages?
10) Describe how the Vendor will ensure all hardware and Software components of the Vendor Hosting infrastructure will be fully supported by their respective manufacturers at all times. All critical patches for Operating Systems, Databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.

2.6. Ongoing Operations For State Hosted Solution

TOPIC 22 - SUPPORT AND MAINTENANCE FOR STATE HOSTED SYSTEMS

The State will evaluate whether the Vendor's proposed support and maintenance plan includes a description of the types and frequency of support, detailed maintenance tasks – including Scheduled maintenance and upgrades, and any other dependencies for on-going support and maintenance of the system. This narrative should reflect current "best practices" for these tasks.

1) Describe how general support and maintenance skills are transferred to State technical support personnel for knowledge sharing.
2) Describe the Database support requirements.

Remainder of this page intentionally left blank.

3) Describe how support and maintenance issues are tracked and prioritized detailing methodology and if any additional Software is required. For all maintenance service calls, the Vendor shall ensure the following information will be collected and maintained:
   a) Nature of the Deficiency.
   b) Status of the Deficiency.
   c) Action plans, dates, and times.
   d) Expected and actual completion time.
   e) Deficiency resolution information.
   f) Resolved by.
   g) Identifying number i.e. work order number.
   h) Issue identified by.
4) Describe any procedures required to handle escalation and emergency calls.
5) Describe how the Vendor will work with the State to identify and troubleshoot large-scale System failures.
6) Describe the Vendor's Change Management policy for notification and tracking of change requests as well as critical outages.
7) Detail the types and frequency of scheduled support and maintenance tasks required.
8) Describe any different levels and or models of support and maintenance that you provide.
9) Describe how you will enable the State to deploy the selected managed service for endpoint detection and response within the State Hosted Server Environment.

Remainder of this page intentionally left blank.

APPENDIX D: STANDARDS FOR DESCRIBING VENDOR QUALIFICATIONS

1. Vendor Qualifications

Vendor qualifications are important factors in selecting Software and accompanying Implementation and Support Services. To facilitate evaluation of Vendor qualifications, the State seeks information about:

a) Corporate qualifications of each Vendor proposed to participate in the Project.

b) Proposed team organization and designation of key staff.

c) Individual qualifications of Candidates for the role of Project Manager.

d) Individual qualifications of Candidates for other key staff roles.

This Appendix identifies specific information that must be submitted with your Proposal.

2. Required Information on Corporate Qualifications

Describe the major business areas of the firm and length of time in business. Provide a high-level description of the firm's organization and staff size. Discuss the firm's commitment to the public sector, experience with this type of Project Implementation and experience in New Hampshire.

2.1. Financial Strength

Provide at least one of the following:

a) The current Dunn & Bradstreet Report on the firm.

b) The firm's two most recent audited financial statements; and the firm's most recent un-audited, quarterly financial statement.

c) The firm's most recent income tax return.

2.2. Litigation

The relevance of involvement of the company in litigation will be considered. Identify and describe any claims made by clients during the last ten (10) years. Discuss merits, current status and, if available, outcome of each matter.

2.3. Prior Project Descriptions

Provide descriptions of no more than Two (2) similar projects completed in the last Five (5) years. Each project description should include:

a) An overview of the project covering type of client, objective, project scope, role of the firm and outcome.

b) Project measures including proposed price, actual project price, proposed project schedule and actual project schedule.

c) Names and contact information (name, title, address and current telephone number) for one or two references from the client.

d) Names and project roles of individuals on the Vendor proposed team for the New Hampshire Project that participated in the project described.

2.4. Subcontractor Information

Vendors must provide information on any Subcontractors proposed to work on this Project. Required information shall include but not be limited to:

a) Identification of the proposed Subcontractor and a description of the major business areas of the firm and their proposed role on the Project.

b) A high-level description of the Subcontractor's organization and staff size.

c) Discussion of the Subcontractor's experience with this type of Project.

d) Resumes of key personnel proposed to work on the Project.

e) Two references from companies or organizations where they performed similar services (if requested by the State).

f) Physical location of Subcontractor's headquarters and branch offices, including offshore locations.

Subcontractors who provide solutions must meet all technical requirements defined in Appendix B.

3. Team Organization and Designation of Key Vendor Staff

a) Provide an organizational chart depicting the Vendor Project Team. This chart should identify key staff required from the Vendor, any Subcontractors, and the State.

b) Define the responsibilities and length of assignment for each of the roles depicted in the organizational chart. Identify the positions that should be designated key staff.

A single team member may be identified to fulfill the experience requirement in multiple areas.

3.1. Candidates for Project Manager and Key Vendor Staff Roles

Although the State recognizes that staff availability is somewhat uncertain, qualifications of the Project Manager are particularly critical. Therefore, the State requires that the Project Manager be identified with some degree of certainty.

For the Project Manager Candidate, and all other Key Vendor Staff Roles, provide a resume not to exceed three (3) pages in length addressing the following:

a) The candidate's educational background.

b) An overview of the candidate's work history.

c) The candidate's project experience relevant to the proposed project, including project type, project role and duration of the assignment.

d) Any significant Certifications held by or honors awarded to the candidate.

e) At least three (3) references, with publicly available contact information that can address the candidate's performance on past projects.

APPENDIX E: PRICING

1. Pricing

Vendor's Price Proposal must be based on the worksheets formatted as described in this Appendix.

The Vendor must assume all reasonable travel and related expenses. All labor rates will be "Fully Loaded", including, but not limited to meals, hotel/housing, airfare, car rentals, car mileage, and out-of-pocket expenses.

1.1. Activities / Deliverables / Milestones Pricing

The Vendor must include the IT service activities, tasks and preparation of required Deliverables, pricing for the Deliverables required based on the proposed approach, and methodology and tools. The following format must be used to provide this information.

Table E-1.1. ACTIVITY / DELIVERABLES / MILESTONES PRICING WORKSHEET

PLANNING AND PROJECT MANANAGEMENT

ITEM #	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PROJECTED DELIVERY DATE	PRICE
1	Project Kickoff Meeting and Kickoff Materials	Non-Software		
2	Detailed Work Plan, Schedule, Deliverables, Dependencies, and Payment Milestones	Written		
3	Project Status Reports and Risk / Issue Log	Written		
4	Infrastructure Plan, including Desktop, Network, Environment, Hosting, and Configuration Requirements	Written		
5	Security Plan and Access Control Design	Written		
6	Communications and Change Management Plan	Written		
7	Software Configuration and Release / Promotion Plan	Written		
8	Systems Interface Plan and Design / Capability	Written		
9	Testing Strategy, Master Test Plan, Scripts, Results, and Defect Management Support	Written		
10	Data Conversion / Migration Plan and Design	Written		
11	Deployment / Cutover / Go-Live Plan	Written		
12	Comprehensive Training Plan, Curriculum, and Training Materials	Written		
13	End User Support Plan	Written		

14	Business Continuity and Disaster Recovery Plan	Written		
15	Documentation of Operational Procedures, Administrator Guide, and Operations Support Guide	Written		

INSTALLATION

ITEM #	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PROJECTED DELIVERY DATE	PRICE
16	Business Process Validation Document	Written		
17	Requirements Traceability Matrix	Written		
18	Solution Design Document	Written		

TESTING

ITEM #	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PROJECTED DELIVERY DATE	PRICE
19	Data Dictionary and Field Mapping Document	Written		
20	Payment Workflow and Reconciliation Design	Written		
21	Role and Permission Matrix	Written		
22	Exception Handling and Manual Workaround Procedures	Written		
23	Production Readiness Checklist	Written		
24	Final Configuration / As-Built Documentation	Written		

SYSTEM DEPLOYMENT

ITEM #	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PROJECTED DELIVERY DATE	PRICE
25	Post-Go-Live Support Plan	Written		
26	Project Closeout / Final Project Summary	Non-Software		

ONGOING OPERATIONS ARE DETAILED IN PRICING TABLES BELOW (do not enter an amount here for ongoing operation. Use the tables below)

PROJECT COMPLETION

ITEM #	ACTIVITY, DELIVERABLE, OR MILESTONE	DELIVERABLE TYPE	PROJECTED DELIVERY DATE	PRICE
31	Conduct Project Exit Meeting	Non-Software		

TOTAL

TOTAL	$

1.2. Software License Pricing

Please utilize the following table to detail the required Software price associated with your Proposal.

Table E-1.2. SOFTWARE LICENSE PRICING WORKSHEET

Item	SOFTWARE ITEM	INITIAL PRICE
1		
2		
3		
Total		

NOTE to Vendor: Key Assumption(s): Vendors should add/use a separate row for each Software License item proposed.

1.3. Software Operations, Maintenance and Support Pricing

Please utilize the following table to provide a detailed listing of the annual operational prices of each Software product that is part of your Proposal, including operations, maintenance and support. This should not include the initial price identified in the Software License Pricing Table listed above.

Table E-1.3. SOFTWARE OPERATIONS, MAINTENANCE, AND SUPPORT PRICING WORKSHEET

SOFTWARE NAME	YEAR 1	YEAR 2	Optional			
			YEAR 3	YEAR 4	YEAR 5	YEAR 6
Total						

NOTE to Vendor: Key Assumption(s): Vendors should add/use a separate row for each Software package proposed that requires annual support prices.

1.4. Hosting Pricing

Please utilize the following table to provide a detailed listing of the annual Hosting prices of the full Application. This may include Web Site Hosting Fee, Technical Support Fee, Maintenance and Update Fees, Data Storage Fees, Upload/Download Fees etc.

Table E-1.4. HOSTING DETAIL PRICING WORKSHEET

HOSTING DESCRIPTION	YEAR 1	YEAR 2	Optional			
			YEAR 3	YEAR 4	YEAR 5	YEAR 6
Total						

NOTE to Vendor: Key Assumption(s): Vendors should add/use a separate row for each Hosting item proposed.

1.5. Other Pricing

If other prices exist but were not handled in the above Pricing Table Worksheets, please utilize the following table to provide a detailed itemization of any additional price.

Table E-1.5. OTHER PRICING WORKSHEET

OTHER PRICE DESCRIPTION	YEAR 1	YEAR 2
Total		

NOTE to Vendor: Key Assumption(s): Vendors should add/use a separate row for each other price item proposed.

Remainder of this page intentionally left blank.

1.6. Implementation Pricing Summary

Please utilize the following table to summarize all Implementation prices associated with your Proposal.

Table E-1.6. IMPLEMENTATION PRICING SUMMARY WORKSHEET

Pricing TABLE #	PRICE TYPE	TOTAL PRICE
1	Activities/Deliverables/Milestones Pricing (Total from Activity/Deliverables/Milestones Pricing Worksheet)	
2	Software License Pricing (Total from Software License Pricing Worksheet)	
3	Software Operations, Maintenance, and Support Pricing (Total from Software Operations, Maintenance, and Support Pricing Worksheet)	
4	Hosting Pricing (Total from Hosting Detail Pricing Worksheet)	
5	Other Pricing (Total from Other Pricing Worksheet)	

TOTAL:	

2. Additional Pricing Reference

Tables E-2.1 through E-2.2 include information for reference purposes only and will not be taken into account in determining the Price Proposal score.

2.1. Vendor Staff, Resource Hours and Rates

Use the Vendor Staff Position, Resource Hours and Rates Worksheet to indicate the individuals who will be assigned to the Project, hours and applicable rates. Information is required by stage. Names must be provided for individuals designated for key roles, but titles are sufficient for others.

Table E-2.1. Vendor Staff, Resource Hours and Rates

Vendor Role	Name	Planning and Project Management	Installation and Testing	System Deployment	Ongoing Operations	Hourly Rate	Hours X Rate
Project Manager							
Position #1							
Position #2							
Position #3							
TOTALS							

NOTE to Vendor: Key Assumption(s): Denote key roles by adding "(key)" to the 'Vendor Role' column. Add as many rows as necessary to complete the full proposed team.

2.2. Future Vendor Rates

The State may request additional services from the selected Vendor and require rates if additional services are required. The following format must be used to provide this information.

The New Hampshire State Fiscal Year (SFY) runs from July 1 of the preceding calendar year through June 30 of the applicable calendar year.

Table E-2.2. FUTURE VENDOR RATES PRICING WORKSHEET

VENDOR ROLE	SFY2027	SFY2028
Project Manager		
Position 1		
Position 2		
etc.		
Total		

NOTE to Vendor: Key Assumption(s): Denote key roles by adding "(key)" to the 'Vendor Role' column. Add as many rows as necessary to complete the full proposed team.

Remainder of this page intentionally left blank.

APPENDIX F: DOIT INFRASTRUCTURE AND SECURITY

The Project will be conducted in cooperation with the New Hampshire Department of Information Technology (DoIT). DoIT coordinates the statewide Information Technology activities.

1. Technical Architecture

Components of the State's technical architecture include:

1.1. State Network Environment

The State of New Hampshire operates a Metropolitan-Area-Network (MAN) in the City of Concord, NH using a combination of leased and owned fiber optic cable. State of New Hampshire locations outside of the Concord, NH main facility are connected via multiple wide-area Networks using various technologies including Carrier Ethernet Services (CES), Microwave Wireless and Virtual Private Networks (VPN) Tunnels over the Internet. State Agency Networks have varying levels of integration and connectivity to the statewide core for resource sharing and centralized administration by the Department of Information Technology (DoIT). State agencies connect to the State's central core Network location in Concord to facilitate access to email, the Internet, and the State's financial Applications. Direct support is provided for twenty-one partner agencies; other State agencies support their own Networks, out-source the support, or use the resources of another agency.

1.2. Internet Access

The State of New Hampshire has purchased through American Registry for Internet Numbers (ARIN) its own External IP Address Range and Autonomous System Number. The State advertises its External IP Space and Autonomous System Number to two different Internet Service Providers to provide failover in the event of a single Internet Service Provider (ISP) Network failure.

1.3. VMware

The State uses VMware for Windows Server virtualization and virtual hosts are deployed at two separate State campus sites. VMware provides a highly scalable and high availability environment for the State's many Agencies. If a virtual host fails, VMware automatically fails over all the virtual Servers on that host to another host. The EMC Networker product is used to manage backups for this environment utilizing Data Domain as the disk-to-disk repository.

1.4. Oracle

For the State's Oracle enterprise systems, an Oracle/Linux solution (OVM) is used for the virtual environment. Similar to the windows environment, this Solution provides a highly scalable and high availability environment and also utilizes the EMC Networker and Data Domain backup solution. Data Domain is also employed to meet the backup requirements within OVM.

2. Future Systems Environment

Future design and development efforts should conform to the emerging environment as defined by the New Hampshire Statewide Strategic Information Technology Plan. This environment is end-user-centric, utilizing the Internet whenever possible, promoting electronic transactions, and centralized common services (security, e-Commerce), where possible.

2.1. Security

The State must ensure that appropriate levels of security are implemented and maintained in order to protect the integrity and reliability of its information technology resources, information, and services. State resources, information, and services must be available on an ongoing basis, with the appropriate infrastructure and security controls to ensure business continuity and safeguard State Networks, Systems and Data.

Remainder of this page intentionally left blank.

APPENDIX G: MERCHANT CARD SERVICES

Applicable

PCI DSS Payment Application Data Security Standard (PA DSS)

Whereas the Vendor provides a Commercial Off-the-Shelf (COTS) product used by the Department of Safety, which transmits, processes or stores cardholder Data and therefore must meet PA-DSS validation requirements

Whereas the Vendor access to the production environment which transmits, processes or stores cardholder data and therefore is considered a "service provider" under Requirement 12.8 of the PCI DSS Requirements and Security Assessment Procedures of the latest edition.

The Vendor agrees to the following provisions:

a) Vendor shall comply with all credit card brand rules, as applicable, in regards to their environment. The Vendor will work with the State if any non-compliance issues occur to ensure proper remediation of any non-compliance issues.

b) Payment Card Industry Security Standards Council (PCI SSC) – Payment Application Data Security Standard (PA DSS) – As the Vendor's product is part of the processing, transmitting or storing of Cardholder Data it is hereby agreed that:

c) Vendor agrees to participate in the Payment Card Security Standards Council (PCI) Payment Application Data Security Standards program (PA DSS);

ii) Vendor agrees to provide evidence of compliance, PA DSS Attestation of Validation prior to Contract approval and upon request;

iii) Vendor is required to provide a PA-DSS Implementation Guide with instructions on secure product implementation, secure configuration specifics, and to clearly delineate vendor responsibilities for meeting PCI DSS requirements. It should detail how to enable security settings within the network; and

iv) Vendor shall immediately notify the NH DoIT Chief Information Security Officer and the Merchant Card Administrator if it learns its application is no longer PA DSS compliant and shall immediately provide the DOIT Chief Information Security Officer of the steps being taken to remediate the non-compliance status. In no event should Vendor's notification to the DoIT be later than seven (7) calendar days after Vendor learns it is no longer PA DSS complaint.

d) PCI DSS Requirement 12.8 of the latest edition, Service Provider – If the Vendor provides Services on the production environment used in the processing, transmission and/or storage of Cardholder Data, it is hereby agreed that:

i) Vendor agrees that it is responsible for the security of all Cardholder Data that it obtains or possesses, including but not limited to the functions relating to storing, processing, and transmitting the Cardholder Data.

ii) Vendor attests that, as of the Effective Date of this RFP, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with PCI DSS.

iii) Vendor agrees to supply the current status of Vendor's PCI DSS compliance, and evidence of its most recent validation of compliance upon execution of this addendum to Department of Safety. Vendor must supply to Department of Safety an Attestation of compliance at least annually and upon request.

iv) Vendor shall immediately notify NH DoIT Chief Information Security Officer and the Merchant Card Administrator if it learns that it is no longer PCI DSS compliant and shall immediately provide Department of Safety the steps being taken to remediate the non-compliance status. In no event shall Vendor's notification to NH DoIT Chief Information Security Officer be later than seven (7) calendar days after Vendor learns it is no longer PCI DSS compliant.

v) Vendor acknowledges that any indemnification provided for under the Contract referenced above applies to the failure of the Vendor to be and to remain PCI DSS compliant.

vi) Vendor shall agree to work with Department of Safety in order to clarify how responsibilities for PCI DSS requirements may be shared, by completing a CPI DSS Responsibility Matrix.

e) Vendor shall disclose any Nested Third-Party Service Provider (TPSP) that is a part of the Cardholder Environment. Vendor shall document the Nested TPSP's allocation of liability, responsibility and costs relating to actions of outsourced contractors and/or notifying the Vendor regarding incidents. Department of Safety shall require an Attestation of Compliance on an annual basis and upon request from the Nested Third-Party Service Provider.

Remainder of this page intentionally left blank.

APPENDIX H: TERMS AND DEFINITIONS

The following general contracting terms and definitions apply except as specifically noted elsewhere in this document.

Term:	Definition:
Acceptance	Notice from the State that a Deliverable has satisfied Acceptance Test or Review.
Commercial Off-The-Shelf Software	Software that is purchased from a vendor and is ready for use with little or no change.
Confidential Information	Information required to be kept confidential and restricted from unauthorized disclosure under the Contract. "Confidential Information" or "Confidential Data" means all private/restricted confidential information disclosed by one party to the other. Confidential Information includes any and all information owned or managed by the State of NH of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes but is not limited to Personal Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.
Data	State records, files, forms, electronic information and other documents or information, in either electronic or paper form, that will be used /converted by the Vendor during the contract term.
Data Breach	"Data Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for another than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Data Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
Deficiency (ies)/ Defects	A failure, shortcoming or error in a Deliverable resulting in a Deliverable, the Software, or the System, not conforming to its Specifications.
Deliverable	Any written, software, or non-software item (letter, report, manual, book, code, or other) provided by the Contractor to the State or under the terms of a Contract requirement.
Documentation	All information that describes the installation, operation, and use of the Software, either in printed or electronic format.
Enhancements	Updates, additions, modifications to, and new releases for the Software or System, and all changes to the Documentation as a result of improvement in quality, value, or extent.
Hosted Services	Applications, IT infrastructure components or functions that organizations access from external service providers, typically through an internet connection.

Term:	Definition:
Hosted System	The combination of hardware, software and networking components used by the Application Service Provider to deliver the Hosted Services.
Identification and Authentication	Supports obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.
Implementation	The process for making the System fully Operational for processing the Data.
Infrastructure as a Service (IaaS)	The Contractor is responsible for ownership and management of the hardware that support the software, including servers, networking and storage.
Non-Public Information	Information, other than Personal Information, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance, agreement or administrative rule from access by the general public as public information.
Open-Source Software	Software that guarantees the user unrestricted use of the Software as defined in RSA chapter 21-R:10 and RSA chapter 21-R:11.
Operational	Operational means that the System is ready for use and fully functional, all Data has been loaded; the System is available for use by the State in its daily operations, and the State has issued an Acceptance Letter.
Personal Information	"Personal Information" (or "PI") or "Personally Identifiable Information" (PII) means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Project	The planned undertaking regarding the entire subject matter of an RFP and Contract and the activities of the parties related hereto.
Proposal	A written plan put forth by a Vendor for consideration in response to a solicitation by the State.
Security Incident	"Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.
Services	The work or labor to be performed by the Contractor on the Project as described in a contract.

Term:	Definition:
Software	All Custom, SAAS and/or COTS Software provided by the Contractor under the Contract.
Software Deliverables	All Custom, SAAS and/or COTS Software and Enhancements.
Software License	Licenses provided to the State under this Contract.
Software-as-a-Service (SaaS)	The capability provided to the State to use the Contractor's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The State does not manage or control the underlying cloud infrastructure including network, servers, Operating Systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Solution	A proposed set of Software and Services addressing the requirements and terms of a Request for Proposal.
Specifications	The written details that set forth the requirements which include, without limitation, this RFP, the Proposal, the Contract, any performance standards, Documentation, applicable State and federal policies, laws and regulations, State technical standards, subsequent State-approved Deliverables, and other specifications and requirements described in the Contract Documents. The Specifications are, by this reference, made a part of the Contract as though completely set forth herein.
State Data	All Data created or in any way originating with the State, and all Data that is the output of computer processing of or other electronic manipulation of any Data that was created by or in any way originated with the State, whether such Data or output is stored on the State's hardware, the Contractor's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Contractor.
State Fiscal Year (SFY)	The New Hampshire State Fiscal Year (SFY) runs from July 1 of the preceding calendar year through June 30 of the applicable calendar year.
Subcontractor	A person, partnership, or company not in the employment of, or owned by, the Vendor, which is performing Services under this Contract under a separate Contract with or on behalf of the Vendor.
Support Services	The maintenance and technical support services provided by Contractor to the State during the Term of the Contract.
System	All Software, specified hardware, and interfaces and extensions, integrated and functioning together in accordance with the Specifications.
Vendor/Contracted Vendor	The company whose Proposal or quote was awarded a Contract with the State and who is responsible for the Services and Deliverables of the Contract.
Verification	Supports the confirmation of authority to enter a computer system application or network.

Term:	Definition:
Warranty Period	A period of coverage during which the Vendor is responsible for providing a guarantee for products and Services delivered as defined in the Contract.
Work Plan	Documentation that details the activities for the Project created in accordance with the Contract. The plan and delineation of tasks, activities and events to be performed and Deliverables to be produced under the Project as specified in Appendix B: Business/Technical Requirements and Deliverables. The Work Plan shall include a detailed description of the Schedule, tasks/activities, Deliverables, critical events, task dependencies, and the resources that would lead and/or participate on each task.

Remainder of this page intentionally left blank.

APPENDIX I: P-37 STATE OF NEW HAMPSHIRE GENERAL PROVISIONS AND EXHIBITS

The P-37 STATE OF NEW HAMPSHIRE GENERAL PROVISIONS AND EXHIBITS contract template is included as ATTACHMENT 1 – Contract Template.

Remainder of this page intentionally left blank.