Revised Schedule

REQUEST FOR PROPOSAL
2020000076

SaaS Billing and Inspection Database

Colorado Department of Public Health and Environment
Procurement and Contracts Unit
4300 Cherry Creek Drive South
Denver, CO 80246

Table of Contents

REQUEST FOR PROPOSALS SIGNATURE PAGE	3
SCHEDULE OF ACTIVITIES	4
SECTION 1: ADMINISTRATIVE INFORMATION	5
SECTION 2: STATEMENT OF WORK	13
SECTION 3: RESPONSE FORMAT	54
SECTION 4: PROPOSAL EVALUATION	56

REQUEST FOR PROPOSALS SIGNATURE PAGE

IMPORTANT:
The RFP Number and RFP Submission Deadline must be on the OUTSIDE of the sealed RFP response.
RETURN THIS PAGE WITH YOUR RESPONSE

RFP INFORMATION			
RFP #:	**2020000076**	TITLE:	**SaaS Inspection and Billing Database**
ANTICIPATED INITIAL CONTRACT TERM:			**One (1) Year**
ANTICIPATED OPTIONAL EXTENSION TERMS:			**Four (4) 1-year extension terms, or a combination of optional extension terms totaling no more than 4 years.**
SUBMIT INQUIRIES & SEALED PROPOSALS TO:			
Colorado Department of Public Health and Environment Procurement and Contracts Unit Mail Room (B1) 4300 Cherry Creek Drive South Denver, CO 80246 Attention: Allan Smith, Senior Purchasing Agent			
Allan Smith, Senior Purchasing Agent			
303-692-2072			
allan.smith@state.co.us			
Submit one (1) Original copy and four (4) paper copies. Instructions regarding submission of an electronic copy are included in the main body of this RFP.			
OFFEROR'S CONTACT INFORMATION			
COMPANY NAME:		CONTACT:	
STREET ADDRESS:		PHONE:	
CITY/STATE/ZIP:		E-MAIL:	
FEIN:		VSS Number	
OFFEROR'S AUTHORIZED SIGNATURE			
AUTHORIZED SIGNATURE:			
PRINTED NAME:		TITLE:	

SCHEDULE OF ACTIVITIES

Solicitation Activity		Time	Date
1.	Solicitation Published on Colorado VSS System **www.colorado.gov/vss**	N/A	9/26/2019
2.	Prospective Offeror's written inquiry deadline. Submit all inquiries by email to Allan Smith @ allan.smith@state.co.us. (**No Questions will be accepted after this Date/Time**)	2:00 PM MDT	10/10/2019
3.	Answers to written inquiries published on Colorado VSS at **www.colorado.gov/vss**	Estimated	10/16/2019
4.	Proposal submission deadline	2:00 PM MDT	~~10/30/2019~~ 11/6/2019
5.	Evaluation Period	Estimated	Week of 11/~~3~~10/2019
6.	Demonstrations	Estimated	Week of 11/1~~0~~7/2019
6.	Estimated Award Date	N/A	Week of 11/~~15~~25/2019

SECTION 1: ADMINISTRATIVE INFORMATION

1.1. ISSUING OFFICE

This Request for Proposals (RFP) is issued by the State of Colorado, Department of Public Health and Environment (CDPHE), Procurement and Contracts Unit, for the benefit of the State of Colorado (State). The CDPHE Procurement and Contracts Unit and Purchasing Agent listed on the RFP Signature Page is the sole point of contact concerning this RFP. All communication must be directed to the designated Purchasing Agent.

1.2. COLORADO VENDOR SELF SERVICE AND REGISTRATION

The State uses the Colorado Operations Resource Engine (CORE) and Vendor Self Service (VSS) to publicly post solicitations.

Solicitation details for goods and services, as well as construction notices, are publicly available without registration on VSS. Any addendum or modification to this RFP will be published using Colorado VSS. Offerors should check VSS on a regular basis. Vendors that are registered on VSS may choose to receive notifications of any new information regarding this RFP.

An Offeror must have a current registration on VSS in order to be awarded under this RFP. There is no cost to register on Colorado VSS. To become a registered supplier on VSS, please visit www.colorado.gov/vss

1.3. INVITATION TO SUBMIT PROPOSALS

CDPHE is posting this RFP on Colorado VSS so that Offerors who have an interest may submit a Proposal in accordance with terms of this RFP. Please read and be aware of the administrative information attached to this RFP. This RFP is intended to provide prospective Offerors with sufficient information to enable them to prepare and submit Proposals for consideration. This RFP contains the instructions governing the Proposal to be submitted and the material to be included therein. All mandatory requirements stated in this RFP must be met to be eligible for consideration.

It is the sole responsibility of the Offeror to ensure that a Proposal is submitted and received prior to the date and time specified on Colorado VSS. Late Proposals will not be accepted.

The State intends to select one or more Proposals for award as a result of this RFP and to contract for the goods or services in such awarded Proposal. The State reserves the right to select Proposals for award as it is deemed to be in the best interest of the State.

1.4. OFFEROR IDENTIFICATION

All Proposals must include a valid tax identification number for the Offeror. Any Offeror must be a legal entity with the legal right to contract in the State of Colorado. Only the identity of the Offeror will be used to determine the Offeror's registration status on VSS. If an Offeror is owned or controlled by a parent

company, the Proposal must also identify the name, main office address, and tax identification number of such parent company.

1.5. Official Means of Communication

Prior to the proposal submission deadline for this RFP, all official communication from the State regarding this RFP, including any modification or addendum, will be posted as a notice on VSS. Offerors should carefully and regularly monitor VSS for any such postings.

At any time prior to the execution of a contract as a result of this RFP, any news release or other contact with media representatives regarding this RFP or any Proposal submitted in response to this RFP is prohibited, to the extent permitted by law, without the prior express written approval of the State.

1.6. Inquiries

Unless otherwise noted, prospective Offerors may make written or electronic mail inquiries concerning this RFP to obtain clarification of requirements. E-mail is the preferred method for Offerors to submit inquiries. No inquiries will be accepted after the date indicated in the Schedule of Activities section of this RFP.

Inquiries must be made to the designated Purchasing Agent using the contact information appearing on the Signature Page for this RFP.

All inquiries must clearly identify the RFP number, and where appropriate, should include references to any relevant RFP section, paragraph, or question number. Please do not use page numbers as references in an inquiry.

Any response to an Offeror's inquiries will be published as a notice on Colorado VSS. Offerors should not rely on any other statements, whether written or oral, that purport to alter any specification or other term or condition of this RFP. Offerors are responsible for monitoring Colorado VSS for publication of notices regarding this RFP.

1.7. Modification or Withdrawal of Proposals

An Offeror may modify a Proposal submitted in response to this RFP prior to the established proposal submission deadline. An Offeror may withdraw a Proposal at any time.

1.8. The State's Rights

The State reserves the right, in its sole discretion, to waive informalities and minor irregularities in connection with any Proposal received.

The State reserves the right, in its sole discretion, to cancel this entire RFP or individual phases or projects at any time, without penalty.

1.9. CERTIFICATION OF INDEPENDENT PRICE DETERMINATION

By submitting a Proposal in response to this RFP, each Offeror certifies, and in the case of a joint Proposal each party thereto certifies as to its own organization, that in connection with this procurement:

a. The prices in the Proposal have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with any other Offeror or with any competitor, other than a joint Offeror;
b. Unless otherwise required by law, the prices which have been quoted in the Proposal have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, directly or indirectly to any other Offeror or to any competitor; and
c. No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit a Proposal for the purpose of restricting competition.

Each person signing the RFP Signature Page of the Proposal certifies that:

a. The signing individual has the legal authority to bind the Offeror organization to the prices and other obligations offered in the Proposal and that the signing individual has not participated, and will not participate, in any action contrary to the certifications above; and
b. The signing individual is not aware of any person connected with the Offeror organization who has participated in any action contrary to the certifications above; and
c. The signing individual will immediately notify the State if the individual becomes aware of any action by any individual or entity contrary to the certifications above.

A Proposal will not be considered for award where any of the certifications above have been deleted or modified. In the event that any Offeror furnishes with the Proposal a signed statement which sets forth in detail the circumstances of any action contrary to the certifications above, the State may accept such proposal only if the State determines that such disclosure was not made for the purpose of restricting competition.

1.10. PROPRIETARY/CONFIDENTIAL INFORMATION

CDPHE recognizes that some elements of a Proposal may contain proprietary or confidential information. An Offeror may request confidentiality of information submitted in connection with a Proposal using the following procedure:

a. The Offeror must submit a written request for confidentiality together with its Proposal.
b. The request must state *specifically* what elements of the Proposal are to be considered confidential and must provide a justification for the request. To the extent that the request includes multiple types of information, the request must include a specific justification for the request as applied to each different type of information requested to be held confidential.
c. Material requested to remain confidential must be separated from the remaining elements of the Proposal and must be readily identified, such as by labeling the pages as "Proprietary/Confidential."

The State will not consider any requests for confidentiality under the following circumstances:

a. All, or substantially all, of a Proposal is requested to remain confidential.
b. Material requested to be kept confidential is co-mingled with other information in the Proposal (i.e., is not separated from the remainder of the Proposal as required above).
c. The request concerns price or rate information, or information that will be included in any resulting contract for the goods or services proposed.

The CDPHE Procurement Official or delegate will make a written determination regarding any request for confidentiality that complies with the requirements above. In the event that CDPHE denies the Offeror's request for confidentiality or determines that a request is not in compliance with the requirements of this RFP, a notice of that determination will be sent to the Offeror. Upon notice of such denial, the Offeror may withdraw its entire Proposal. An Offeror's decision to allow its Proposal to remain under consideration will be considered acceptance of CDPHE's determination regarding confidentiality.

Nothing in this section prohibits CDPHE from unilaterally determining that any portion of a Proposal should remain confidential, provided that the same criteria for such determination are applied to all proposals submitted under this RFP.

1.11. RFP RESPONSE MATERIAL OWNERSHIP

All material submitted regarding this RFP becomes the property of the State of Colorado. As such, except as provided regarding confidential or proprietary information above, the State of Colorado has the right to use any or all such information or material. The State of Colorado may retain or dispose of all such information or material as is lawfully deemed appropriate.

Except as provided regarding confidential or proprietary information above, all proposals may be reviewed by any person after a Notice of Intent to Make an Award has been issued, subject to the terms of the Colorado Open Records Act ("CORA"), §§24-72-200.1, *et seq.*, C.R.S. Offeror expressly agrees that the State of Colorado may use the materials for all lawful State purposes and may make the information available to the public in accordance with the provisions of CORA.

1.12. PROPOSAL PRICING AND BUDGET

Price and cost information included in any Proposal must be firm, must be stated in U.S. dollars, and must include all related costs (e.g. surcharges, travel, etc.). Estimated Proposal prices are not acceptable. Any costs not included as part of the Proposal may be disallowed under the contract with the awarded Offeror.

Quantities stated in this RFP or in any Proposal are estimates only. Unless expressly stated otherwise, no volume of goods or services to be purchased can be guaranteed. Pricing may be tiered, but may not be contingent upon any unstated assumptions regarding quantities to be purchased.

At the request of the State, Best and Final Offers may be considered in determining the awarded Offeror. Proposals, including Best and Final Offers, Should be firm for a period of not less than one hundred eighty (180) calendar days from the date of award.

CDPHE's budget for this project is between $200,000 and $250,000. This includes the cost of the initial system implementation (all necessary hardware, software, and services to fulfill the requirements of this RFP), but excludes the cost of future annual software maintenance. The total Contract term, including any subsequent annual maintenance periods, Should l not exceed five years.

1.13. TAXES

The State of Colorado, as a purchaser, is exempt from all Federal excise taxes under Chapter 32 of the Internal Revenue Code (Registration No. 84-730123K) and from all state and local government use taxes under §39-26-114(a), C.R.S. The State of Colorado's State and Local Sales Tax Exemption Number is 98-02565.

Goods and services purchased by an Offeror may be subject to sales tax in certain jurisdictions even though the Offeror is purchasing such goods or services in connection with providing goods or services to the State. Any taxes to which Offeror may be subject will not be reimbursed by the State.

1.14. INSURANCE

Any awarded Offeror Should obtain and maintain at all times during the term of any contract resulting from this RFP insurance in the kinds and amounts outlined in the Model Contract or Purchase Order Terms and Conditions attached with this RFP.

1.15. CONTRACT TERM

Any contract resulting from this RFP will be effective upon approval by the State Controller or designee, or as otherwise allowed by law. The contract performance should commence upon the effective date of the contract and should be undertaken and performed in the sequence and manner set forth in the contract. The estimated total term of any resulting contract is stated on the Signature Page for this RFP. CDPHE reserves the right to extend or modify contract dates.

1.16. CONTRACTUAL OFFER AND ACCEPTANCE

1.16.1. Acceptance or Rejection of RFP and Contract Terms

By submitting a Proposal, Offeror acknowledges and accepts all terms and conditions of this RFP unless Offeror's proposal clearly and unequivocally rejects such term or condition. Failure to clearly articulate any such rejection, or any variation between a Proposal and this RFP, Should be deemed a waiver of any rights to subsequently modify the terms of performance. Rejection of any term or condition of the RFP may be grounds for the state to reject a Proposal or decline to select a Proposal for award.

A Proposal signed by an authorized representative for the Offeror and submitted in response to this RFP Should constitute a binding offer for the State to purchase or otherwise contract for the goods or services proposed therein. Except as modified herein or as agreed to by the State, the Model Contract or Purchase Order Terms and Conditions included with this RFP will be binding upon the awarded Offeror. The contents of the Proposal, including the services of any persons specified, will become contractual obligations of the awarded Offeror if a contract ensues. Failure of the awarded Offeror to accept these obligations in a

resulting contract may result in cancellation of the award and such Offeror may be removed from future solicitations.

1.16.2. Proposed Changes to Contract Terms

A Proposal may include proposed changes to the Model Contract language or Purchase Order Terms and Conditions. Each proposed change must include proposed alternative or substitute language. Such proposed changes will not be viewed as rejections of the RFP terms and conditions. General objections or objections indicated to be negotiated subsequent to the award will not be accepted. The State of Colorado, in its sole discretion, may accept or reject proposed changes during the contract negotiation process with the awarded Offeror. The State's rejection of any proposed change will not alter the awarded Offeror's obligation to perform subject to the terms of this RFP.

The State of Colorado reserves the right to modify the contract language in response to legislative, budget, or policy changes, or as otherwise required by law. The State reserves the right to clarify terms and conditions not having an appreciable effect on quality, price/cost, risk, or delivery schedule during post-award formalization of the contract.

1.17. AGREEMENT EXECUTION

An awarded Offeror should have no longer than forty-five (45) calendar days to enter into a contract after being notified of the award by the State. If no contract has been executed after forty-five days and such delay is not the fault of the State, the State may elect to cancel the award. The State may elect to grant the award to the next most responsive Offeror.

The State of Colorado Should not be liable for any costs incurred by any Offeror prior to the execution of a contract. No property interest of any nature should accrue until a contract is approved by the parties and by the State Controller, or otherwise legally executed as allowed by law.

1.18. INFORMATION SECURITY

All Proposals will be evaluated, in part, based on the Offeror's willingness and ability to comply with all applicable laws, regulations, rules, policies, procedures, or other requirements concerning the safeguarding of any and all State systems and data. The awarded Offeror will be expected to comply with:

a. All Colorado Office of Information Security (OIS) policies and procedures which OIS has issued pursuant to §§24-37.5-401 through 406, C.R.S. and 8 CCR §1501-5 and posted at http://oit.state.co.us/ois
b. All information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any industry standards or guidelines, as applicable based on the classification of the data relevant to Contractor's performance under the Contract. Such obligations may arise from:
    i. Health Information Portability and Accountability Act (HIPAA)
    ii. IRS Publication 1075
    iii. Payment Card Industry Data Security Standard (PCI-DSS)
    iv. FBI Criminal Justice Information Service Security Addendum

v. CMS Minimum Acceptable Risk Standards for Exchanges
vi. Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration

The Awarded Offeror should implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards and guidelines applicable to the performance described in the Proposal.

As a condition of the execution of a contract as a result of this RFP, the Awarded Offeror must provide the State with information reasonably required to assess the Awarded Offeror's ability to comply with the requirements stated above. At the direction of the Office of Information Security ("OIS"), such access and information may include:

a. The results of security audits, penetration tests, or vulnerability scans, as requested by OIS or its designee at any time under this Contract;
b. A recent SOC2 Type II audit including, at a minimum, the Trust Principles of Security, Confidentiality, and Availability, or an alternative audit acceptable to OIS.

1.19. COOPERATIVE PURCHASING

Consistent with CDPHE's obligations under §24-37.5-106(1)(h), C.R.S., any contract resulting from this RFP Should be a cooperative purchasing agreement, pursuant to §24-110-201, C.R.S. CDPHE will be the primary State party to the contract pursuant to §24-37.5-105(3)(i), C.R.S. All Executive Branch State Agencies, any participating Legislative or Judicial Branch State Agencies, and any participating State Institution of Higher Education Should be eligible to purchase the goods or services described in the Proposal and any contract resulting from this RFP.

1.20. RESOLUTION OF CONTROVERSIES

Any controversy in connection with this solicitation or the award of a contract as a result of this RFP Should be resolved according to the provisions of Article 109, Title 24, C.R.S.

1.21. CONFLICT OF INTEREST DISCLOSURE

Offerors must disclose any potential conflict of interest in connection with a Proposal. A conflict of interest may include, but is not limited to, access to any non-public information regarding the RFP or the subject matter of the RFP by the Offeror, or any of the Offeror's employees, contractors, or agents, including any individual who may have had access to non-public information in a prior capacity before entering into a relationship with Offeror.

No individual or entity engaged by the State to prepare this RFP or that has otherwise had prior access to the solicitation or to sensitive information related to this procurement process (including, but not limited to the requirements, statement of work, or evaluation criteria), will be eligible to submit or participate in a Proposal in response to this RFP.

If the State determines that a conflict of interest exists, the State, in its sole discretion, may reject any Proposal or cancel the award of a contract. In the event the Awarded Offeror was aware of any conflict of interest prior to the award of the contract and failed to disclose the conflict to the State, the State may terminate the contract for cause.

The provisions of this section regarding disclosure of conflicts of interest to the State must be included in any subcontracts in connection with performance of the work. The language included in any subcontract must preserve the State's rights to disclosure of conflicts of interest and to termination of the contract on the basis of any unacceptable conflict or failure to disclosure any conflict.

1.22. COLORADO BUSINESS REGISTRATION

Within ten (10) business days of the notification of the award of a contract under this RFP, the awarded Offeror be properly registered with the Colorado Secretary of State's Office to do business in Colorado. The State may request that the awarded Offeror provide evidence of such registration, as well as other organizing documents such as Articles of Incorporation or By-laws.

SECTION 2: STATEMENT OF WORK

This section provides the Offeror with a general overview of the requirements contained within this RFP. Additional information regarding the specific requirements may be contained in any documents attached to this RFP.

2.1. KEY TERMINOLOGY

Whenever the following terms are in this document, they have the meaning as outlined below:

a. **"Acceptance Criteria"** means the standards listed in an order which characterize the Authorized Purchaser's specific requirements and conditions that must be satisfied by the MSP for the Authorized Purchaser to accept the completed Deliverables.
b. **"Acceptance Testing"** means testing as described in a Purchase Order to be performed by MSP to determine that deliverable(s) meet the Acceptance Criteria.
c. **"Awarded Offeror"** means the Offeror(s) whose proposal response the State deems to be most advantageous considering price and the evaluation factors set forth in this RFP.
d. **"Business Day"** means 8:00 a.m. to 5:00 p.m., Mountain Time, Monday through Friday, excluding State holidays and State mandated office closures.
e. **"Contractor"** means the Awarded Offeror following the execution of a Contract resulting from this RFP.
f. **"Deliverables"** means the outcome to be achieved or output to be provided, in the form of a tangible object or software that would be produced as a result of Offeror's Work as described in a Proposal.
g. **"Delivery Schedule"** means the schedule(s) for the performance of Work, as set forth in an Order that lists: (1) each Deliverable, including its measurable attributes; (2) payment schedule within each Deliverable, including milestone completion date; and (3) final delivery date for each Deliverable.
h. **"Documentation"** means an operational description, in written format, of all Work to be performed under an Order, including documents that are Deliverables.
i. **"Errors"** mean defect(s) in the Deliverables, Work, or Work Product such that the Work or Work Product does not comply with the specifications set forth in an Order.
j. **"Final Acceptance"** means the date upon which provides MSP written notice that it has accepted all the Work to be performed, including all Deliverables or when applicable the System to be delivered, including any updates, corrections, or additions to content, and that will make payment for Work performed. The Warranty Period Should commence upon Final Acceptance.
k. **"Key Persons"** means the State Staff (supervisor or project manager) who will be principally responsible for managing the Services or for performance of Work under an Order and the satisfactory completion, delivery and acceptance of the related Deliverables.
l. **"MWBE"** means a Minority or Women-owned Business.
m. **"Offeror"** means any entity or individual submitting a proposal in response to this RFP.
n. **"Open Source Software"** means one or more of the following: (1) any software that contains or is derived in any manner (in whole or in part) from open source software or software subject to similar licensing or distribution requirements; and (2) any software that requires as a condition of its use, modification or distribution that such software (or other software

incorporated into, derived from or distributed with such software) be either (a) disclosed or distributed in source code form; (b) licensed for the purpose of making derivative works; or (c) redistributable at no charge.

o. **"Proposal"** means an Offeror's response to this RFP. A Proposal may also be called a bid, response, or offer. If such have been requested and submitted following initial responses, an Offeror's Proposal Should include any clarifications or any best-and-final offer.

p. **"Request for Proposals"** or **"RFP"** means a procurement solicitation that seeks offers from organizations or individuals to perform the scope of work defined in the RFP, in accordance with the terms listed in the RFP. An RFP is issued with the intent of selecting the most advantageous proposal, making an award to that Offeror, and entering into a contract.

q. **"Solicitation"** means a document issued by the State of Colorado agency that requests competitive offers from organizations or individuals to sell the goods or services that are specified in the document. A solicitation typically results in an award of a contract or purchase order for the goods or services, based on an award methodology defined in the solicitation. Types of solicitations include: Requests for Proposals (RFPs), Invitation for Bids (IFBs) and Documented Quotes (DQs).

r. **"State"** means the State of Colorado.

s. **"Statement of Work"** means the components of an Order that include but are not limited to an introduction, project objectives, definitions, detailed tasks (and subtasks if needed), measurable Deliverables that correlate with tasks, acceptance criteria, delivery and payment schedule.

t. **"System"** means one or more of the Authorized Purchaser's integrated computer software application and database systems that may be modified, converted, created or enhanced by Contractor for Authorized Purchaser under an Order. System includes but Should not be limited to all related technical design documents, software, databases, database schemas, formats, documentation, reports, memoranda, studies, plans, designs, specifications, statements, drawings, materials, exhibits, schedules and other documents or materials, in whatever media, developed by a contractor in the performance of Work under an Order, as more fully described and specified in a Statement of Work.

u. **"Vendor"** means any organization or individual that seeks to provide, or is already providing, goods or services.

v. **"VSS"** means The State of Colorado's Vendor Self Service Web site. All solicitations published by State agencies and institutions are published on VSS.

w. **"Work"** means all work to be performed under an Order, as more fully described in the Exhibits, schedules, and Statements of Work, including but not limited to: related services that support computer software, data processing, know-how transfer, enhancements, business process automation systems, planning, programming, construction, analysis, design, development, project management, testing, risk analysis, quality assurance, integration, training or implementation.

x. **"Work Product"** means every invention, modification, discovery, design, development, customization, configuration, improvement, process, software program, work of authorship, documentation, formula, datum, technique, know-how, secret, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registrable under copyright or similar statutes or subject to analogous protection) that is specifically made, conceived, discovered, or reduced to practice by a contractor or their agents (either alone or with others) pursuant to an Order.

ACRONYMS

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ADFS	Active Directory Federation Services
ANSI	American National Standards Institute
API	Application Program Interface
BAFO	Best and Final Offer
CCR	Code of Colorado Regulations
CDPHE	State of Colorado Department of Public Health and Environment
CIS	Center for Internet Security
CORE	Colorado Operations Resource Engine
COTS	Commercial Off-the-shelf
CSS	Cascading Style Sheets
DEHS	Division of Environmental Health and Sustainability
DR	Disaster Recover
FTP	File Transfer Protocol
GPS	Global Positioning System
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAD	Information Assurance Directorate
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPHA	Local Public Health Agency
MAC	Media Access Control
MOTS	Modified Off-the-shelf
NAS	Network-attached Storage
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODBC	Open Database Connectivity
OIT	Colorado Governor’s Office of Information Technology
OS	Operating System
OWASP	Open Web Application Security Project

Acronym	Definition
PaaS	Platform as a Service
PII	Personal Identifiable Information
RFC	Request for Comments
RFP	Request for Proposal
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SDL	Security Development Life-cycle
SFTP	Secure File Transfer Protocol
SOW	Statement of Work
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
UAT	User Acceptance Testing
VSS	State of Colorado Vendor Self Service
W3C	World Wide Web Consortium
XML	Extensible Markup Language

2.2. INTRODUCTION

The Colorado Department of Public Health and Environment (CDPHE), Division of Environmental Health and Sustainability (DEHS) is seeking proposals from qualified Offerors to provide a solution for a Software as a Service ("SaaS") Inspection and Billing Database ("Solution").

CDPHE is seeking to implement a browser-based solution which provides automated support to its business processes and promotes improvements to program efficiency, effectiveness, data quality, and security. The core business processes any solution should support are:

1. Licensing of food establishments, food manufacturers, dairies, and animal feeding operations;
2. Inspection of establishments to assure safe restaurants, schools, and child care facilities; assure safety of food from production to consumption; and protect land, water, and air quality resources affected by the animal feeding industry;
3. Maintenance of licensing and inspection data, review of records, and printing of documentation both in the field and in the office;
4. Complaint processing, including receipt of complaints via a standard format and tracking of follow-up and resolution;
5. Billing and managing payment of fees;

6. Customer and public online access;
7. Communication and data support for responses to foodborne illness;
8. Analysis and reporting of program data; and
9. Outreach and education.

CDPHE is seeking to acquire a proven software solution that meets the specific requirements outlined in this RFP. Any solution should also support data access, data entry, and public access.

2.3. BACKGROUND

The Division of Environmental Health and Sustainability (DEHS) is a division of the Colorado Department of Public Health and Environment (CDPHE). The division consists of the Administration & Business Services Unit, the Institutions & Emerging Programs Unit, the Sustainability Programs Unit, the Environmental Agriculture Program, the Retail Food Safety Program, the Milk and Corrections Programs Unit, and the Manufactured Food Safety Program. The Administration & Business Services Unit provide budgets, accounts payable/receivable, and information technology support for all of the other units. The division delivers services that assure safe restaurants, schools, and child care facilities; assures the safety of food from production to consumption; maintains acceptable conditions in state correctional and tanning facilities; protects land, water, and air quality resources affected by the animal feeding industry; and protects and improves Colorado's environment through programs that conserve and reuse resources, prevent pollution, and advance the principles of sustainable development.

All DEHS programs, except the Sustainability Unit, utilize the current DEHS data management solution, which is an externally hosted, web-based application with a portable Field Client to allow for inspections without internet access. The system is maintained by the vendor, but the division owns the data. Many of the programs use the current database, as well as G Suite, Microsoft Office applications, and Microsoft SharePoint to customize reports and to track compliance inspections that are otherwise not available in the current database.

2.4. MANDATORY MINIMUM REQUIREMENTS

In order to submit a proposal for this RFP each Offeror must provide verifiable evidence that the following mandatory requirements are met. Proposals not meeting the minimum requirements will not be further evaluated.

2.4.1
Offeror must have an online/offline field inspection application based program that is completely functional and field tested at the time of RFP submission.

2.4.2
Offeror must have a fully functional and implemented public facing portal solution that allows for:

2.4.2.1 Inspection reports viewing by anonymous users (not needing a login to use)
2.4.2.2 Registered uses to submit new applications for requests for services and submit payments for billed invoices.

2.5. OVERVIEW AND STATEMENT OF WORK SUMMARY

This section contains the details of the scope and deliverables that the Offeror should produce. To fulfill Section 2.5 of the RFP, the Offeror shall provide a detailed response on how these requirements will be met. If the software solution is not capable of meeting each of the requirements, please indicate the additional cost that will be incurred, along with any increase in time to deliver the specific requirement(s).

2.5.1. Non-Functional Requirements

These requirements express some of the attributes of the solution, attributes of the system environment, and requirements of the solution Offeror. They are not necessarily related to a specific business function or functional requirement, but instead, the behavior of the system as a whole.

2.5.1.1. Infrastructure

2.5.1.1.1. Infrastructure – General

ID	Requirement
N.1.1.1	Describe how your solution will utilize a system architecture that is non-vendor proprietary, portable, and will use published APIs.
N.1.1.2	Describe your solution's ability to be adaptable and use extensible architecture for future expansion and scalability without the need for architectural modifications.
N.1.1.3	Document how your solution will provide robust system diagnostics.
N.1.1.4	Describe your strategy for a clustered and load-balanced environment.
N.1.1.5	Describe your capability of supporting production, test, training, and development environments.
N.1.1.6	Describe your solution's user interface response time. Response should be two seconds or less. Describe how the solution will meet this response requirement as well as methods for verification of performance.
N.1.1.7	Document your solution architecture (Identify and justify the classification) for the following: 1. Software as a Service (SaaS); 2. Platform as a Service (PaaS); 3. Infrastructure as a Service (IaaS); 4. Private Cloud (IaaS); 5. Hybrid Cloud (private and public); 6. Hosted Application or Architecture; 7. Physical Infrastructure Architecture; 8. Commercial Off-the-shelf (COTS); 9. Modified Off-the-shelf (MOTS); or 10. Custom architecture, With an understanding that architectures more in compliance with OIT's "Cloud First" initiative are preferred.
N.1.1.8	Provide an architectural overview detailing the necessary components of the system provided, from critical to periphery, with third-party components demarked and identified. Any proposed architecture should include a previous experience reference and performance characteristics (target and present day, if available).

N.1.1.9	Document how your solution will be open and non-proprietary whenever possible, with options available without contract penalty (third-party hardware and software components). Any proprietary components should be noted in the architectural overview, with supporting documentation such as license restrictions, copyright, patent, or similar intellectual property documentation.
N.1.1.10	Describe how your solution is scalable and expandable. Specifically, the system's capability to support a performance of 1000 concurrent transactions with no greater than a two second response time and/or two second transaction time, to create, query, update, or delete owner records. These performance constraints include only system processing time, not human-computer interaction time manipulating the user interface. A description of each system component configuration and its ability to meet the availability and performance specifications should be provided, including strategies for expected increases in throughput and workload over the lifetime of the proposed solution.
N.1.1.11	Describe your solution's capabilities for reporting performance metrics useful to capacity provisioning and diagnostics.
N.1.1.12	Describe your capability to provide a description of the backup, recovery, and disaster recovery (including identifying diminished capacity under disaster) operational characteristics. At minimum, a recommendation for backup and disaster recovery (DR) should be provided, with more mature planning including identification of diminished capacity under DR condition and instructions detailing paths to full operation.
N.1.1.13	Describe your solution regarding custom software development; identify ownership, maintenance, and liability boundaries with respect to code. For example, if the solution uses a "basecode" or "core" solution to which "extensions" as "site code" are added (as in the case of MOTS), the relationship of all code regions with respect to development and support should be detailed.
N.1.1.14	Describe your solution to operational production availability, including maintenance windows, should be no less than 99.9% on a 24-hour x7-day basis. Availability should be considered synonymous with uptime. The solution should require physical hardware, solution reliability, the probability of the solution (including all subcomponents) performing adequately under normal operating conditions for any given one year period, consistently exceed 90% for the purposes of hardware replacement planning. The mean time between failures of any and all components of the solution should always be in excess of 180 days, including series or parallel failure (including redundancy). A description and/or justification of how the solution will meet these requirements Should be included.
N.1.1.15	Provide details of the proposed solution on physical hardware.

2.5.1.1.2. Hardware

ID	Requirement
N.1.2.1	Describe your solution to use open standards for interfaces such as HTML5, XML with third-party hardware, and software components through open architecture.
N.1.2.2	Document your solution's user interface strategy, their futures, their currently supported interfaces and their user interface roadmap.
N.1.2.3	Document your solution's ability to provide a description of each system configuration and its ability to meet the availability specification. Include a system diagram, previous experience achieving these performance specifications, and options in SOW.
N.1.2.4	Document your solution's design to support the capacity requirements to accommodate increases in DEHS throughput and workload over the lifetime of the solution.
N.1.2.5	Describe any hardware used to open architecture with options available without contract penalty (third-party hardware components).

2.5.1.1.3. Interfaces

ID	Requirement
N.1.3.1	Describe your solution or strategy to utilize separate environments for development, testing, and staging prior to production, with the appropriate isolation between. Provide documentation regarding the promotion of code through environments and the use of obfuscated data is strongly recommended.
N.1.3.2	Describe your solution to allow for module expansion, and further for the compartmentalization of legislative-necessitated changes. It should be possible to enable business intelligence at a particular time and day based on legislative constraint, and disable in case of repeal.
N.1.3.3	Describe your solution to include or interface with a GPS system (i.e. Facility location data will be passed from the system to an outside mapping application such as Google Maps). This is desired for data analysis, to support scheduling of tasks, and the creation of maps for planning inspections.

2.5.1.2. Applications

2.5.1.2.1. Applications - General

ID	Requirement
N.2.1.1	Document that your solution conforms to all of the Colorado Information Security Policies pertaining to access control found at http://oit.state.co.us/ois/policies

N.2.1.2	Describe how your solution requires users to log on to the system through Directory and cross-domain authentication. The solution should generally support one user, system-wide. This sign on should include, at a minimum: 1. User classification or role; and 2. Password.
N.2.1.3	Document how your solution allows for the ability to change password at setup, at sign-on, and during the course of a logged-in session.
N.2.1.4	Describe how your solution provides a means for users to recall or reset their password using techniques including, but not limited to: 1. Forgot My Password techniques used extensively on Internet sites; 2. Challenge question and answers established during user setup; 3. If the user successfully answers the challenge question, provide a temporary complex password and require a new password upon successful session sign-on; or 4. Ability for the service desk or authorized designee to reset a password if necessary.
N.2.1.5	Document how your solution is to be configured such that users are notified of impending password expiration. If a user's password has expired, the system should prompt the user to change the password at sign-on.
N.2.1.6	Describe how your solution will provide system administrators the ability to easily configure and update user roles while the system is online.
N.2.1.7	Document your solution's ability to have a single centralized repository for users and their access information (authentication, authorization, and accounting, also referred to as AAA) so that users have one username and one set of authentication credentials (such as a password) and that all user attributes and authorization are managed in one place, including date of entry. This may be accomplished by using a Lightweight Directory Access Protocol (LDAP) server.
N.2.1.8	Document your solution's ability to automatically log off users that have been inactive for a specified period of time. Users can simply sign back on to the system to resume activity from the point of timeout.
N.2.1.9	Describe your solution's ability to support Web services that comply with the OIT Web Services (the current version is the 2012v1 standard).
N.2.1.10	Describe your solution's ability to support the use of pointing devices, hot keys, key combinations, buttons, touch screens, and hyperlinks.
N.2.1.11	Field and screen validation: 1. Describe how your solution provides a visual distinction between mandatory and non-mandatory fields. 2. Describe how your solution provides field validation of data upon entry of the screen for posting.

	3. Describe how your solution provides screen validation upon submission. 4. Describe how your solution displays errors on the appropriate screen for the user.
N.2.1.12	Document how your user applications and how they are browser-based and utilize best-of-breed form design and usability elements.
N.2.1.13	Provide solution details regarding user application screens being printable to configurable local or networked printers, using print commands provided by the browser. The solution's user application screens should be able to be captured using commands provided by the browser.
N.2.1.14	Provide solution details that support the import or export of descriptor tables for DEHS use for other systems.

2.5.1.2.2. End User Client

ID	Requirement
N.2.2.1	Describe how your solution is to be installed as an application on client computers, the minimum and recommended desktop requirements (hardware configuration, software compliment) be specific with purpose clearly identified. Describe how the client solution runs on a 32-bit environment, upgradeable to a 64-bit environment. The solution should be capable of running on a tablet environment running a Microsoft OS. If the solution can be made as a ThinApp, or otherwise served by Thin Clients, it should be noted.
N.2.2.2	Describe your solution's ability to be browser-based, the compatibility (both name and version) and any additional client-side controls, apps, or other executable components should be disclosed. At minimum, current versions of Microsoft Edge, Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome are to be supported, ideally without additional plugins or add-ons. The latest browser benchmark/standards versions should be applied at the time of the deployment and throughout the support life-cycle.
N.2.2.3	Describe your solution's ability to include a means for data to be captured in both online and offline modes (connected/disconnected).
N.2.2.4	Describe your solution's ability to accommodate Mobile/Handheld devices or laptops used by the inspectors in the field. The solution should have the ability to download and save facility data to access when they are not connected to the internet. The devices should have the capability to use all of the necessary functionality of the solution while in disconnected mode. All information gathered while out in the field should be synced to the system the next time the device is connected to the internet.

2.5.1.3. User Interface

2.5.1.3.1. User Interface - General

ID	Requirement
N.3.1.1	Describe your solution's ability to include a browser-based user interface. If the system requires the use of a Web browser, it must meet the OIT standards for Web Browsers. Currently CDPHE uses Windows Internet Explorer 11, the most current version of Microsoft Edge, and the most current version of Google Chrome. The latest browser benchmark/standards versions should be applied at the time of the deployment and throughout the support life-cycle.
N.3.1.2	Describe your solution's ability to provide users with a highly integrated set of application modules offering a consistent user interface in order to minimize user training and system administration.
N.3.1.3	Describe your solution's ability to provide standard GUI items, such as drop-down menus, to make selection easier for frequently used fields, such as form names, commands, and all code tables. The solution should allow for adding/updating items in the drop-down menu.
N.3.1.4	Describe your solution's ability to support "auto complete" functionality for code table lookups as the user begins to enter data in the code table lookup field.
N.3.1.5	Describe your solution's ability to support automated updates to the user application, appropriate to the solution.
N.3.1.6	Describe your solution's ability to support pre-fill fields in appropriate pre-formatted screens, eliminating redundant data entry and without impacting the usability.
N.3.1.7	Document your solution's ability to provide help menus.
N.3.1.8	Describe your solution's ability to allow users to move forward and backward to complete data fields.
N.3.1.9	Describe your solution's ability to allow users to correct spelling errors without having to retype the entire field.
N.3.1.10	Describe your solution's ability to provide users with standard form navigation and allow easy movement from one work area to another via mouse or keyboard.
N.3.1.11	Document your solution's ability to provide default, configurable values for fields based on previous input, referential lookup, or other mechanisms. It should incorporate currently used defaults.
N.3.1.12	Describe your solution's ability to provide lookup tables for valid values for fields.
N.3.1.13	Describe your solution's ability to allow authorized users to configure tables.
N.3.1.14	Describe your solution's ability to translate codes to U.S. English-language words or phrases on the output screen and reports for all codes used.

2.5.1.3.2. User Interface - CDPHE

ID	Requirement
N.3.2.1	Describe how your solution provides all of the information required in a flexible and easy to navigate format and allows easy navigation from field to field and from one application to another.
N.3.2.2	Describe how your solution supports robust editing and validation routines for all mandatory fields, including clearly indicating data that fails validation.
N.3.2.3	Describe how your solution allows navigation from one field to another using “hot keys” for data entry (e.g., Control key shortcuts for save, copy, cut, paste, etc.).
N.3.2.4	Describe how your solution supports, where applicable, the ability to execute multiple transactions in the same screen or session.
N.3.2.5	Describe how your solution provides a visual distinction between mandatory and optional fields during data entry, where both field and page/screen/window validations occur prior to posting/submission for processing. Data entry validation errors should be presented to the user in a form and method appropriate to identify and correct each specific error.
N.3.2.6	Describe your solution’s ability to implement a consistent look-and-feel, including cognitive ergonomics, workflow progression and complexity in order to minimize training and maximize intuitive user interaction.
N.3.2.7	Document Common user interface “best practices” to be used, particularly those as identified in “The Elements of User Experience: User-Centered Design for the Web and Beyond,“ by Garrett, and “Information Architecture for the World Wide Web: Designing Large-Scale Web Sites,” by Morville and Rosenfeld.
N.3.2.8	Describe how your solution, when practical, complies with: HTML5, CSS, JavaScript (W3C); Section 508 of the U.S. Rehabilitation Act, the Americans with Disabilities Act of 1990, or at minimum, be compatible with screen readers (both the site and any downloadable artifacts), be capable of displaying large fonts, and have content context that does not rely on color alone.

2.5.1.4. Security and User Access

2.5.1.4.1. Security

ID	Requirement
N.4.1.1	Describe how your solution follows all OIT policies and OIT Gating Process; enforces security controls based on data classification and secure login; provides security events, handling, and ongoing patching (application databases and systems); utilizes secure protocols and services; and supports an OIT host-based endpoint security solution. The solution must comply with the following security standards: 1. OIT Security Policies (available online at http://oit.state.co.us/ois/policies)

	2. NIST 800-122 “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);” 3. NIST 800-95 “Guide to Secure Web Services;” 4. NIST 800-53 “Recommended Security Controls for Federal Information Systems and Organizations;” 5. The Open Web Application Security Project (OWASP) Development guide; 6. ISO/IEC 17799:2000; 7. Microsoft Security Development Life-cycle (SDL); and 8. CIS Security Benchmarks.
N.4.1.2	Describe your Incident reporting/response procedures and how are they identified and documented.
N.4.1.4	Describe how your solution conforms to all of the Colorado Cyber Security policies pertaining to access control.
N.4.1.5	Describe how your solution provides for the secure remote (connecting to the solution via a network not within the State of Colorado’s control or influence) access of, at minimum, 250 concurrent users, with the appropriate permissions and privileges associated with their account role.
N.4.1.6	Describe how your solution specifies physical infrastructure; a provision must be in place for physical security of all component devices.
N.4.1.7	Describe your solution’s response plan for a security breach in either application code or hosted environment and should integrate with applicable state-operated facilities, datacenter, or security policies.
N.4.1.8	Describe how your solution includes detection and mitigation strategies for security mechanism failure (such as SSL certification expiration, account lockout during session, etc.).
N.4.1.9	Describe how your solution is capable of both code and data quarantine.
N.4.1.10	Describe how you perform regular auditing of security control, including any third-party components or vendor services. Independently verified security controls are preferred.
N.4.1.11	Describe how your solution allows for, at minimum, 250 concurrent users, uniquely auditable and traceable for all transactions regardless of interface (web or desktop client, remote user, etc.)
N.4.1.12	Describe how your solution includes system health tools, to verify and troubleshoot performance.
N.4.1.13	Describe how your solution includes file/data integrity evaluation and recovery capabilities beyond backup and selective recovery.

N.4.1.14	Describe your processes surrounding promotion of application through development, test, staging, and production environments should include authorization procedures.
N.4.1.15	Describe how you warrant against known viruses, malicious software, and backdoor access for a period of 12 months post-delivery. There should be no ability for agents to access data without authorization from the State of Colorado subsequent to the delivery of solution.
N.4.1.16	Describe how you perform or verify the performance of background checks on all workers, including third-parties, subcontractors, and vendor service providers.
N.4.1.17	Describe your solution's ability to make the use of encryption for all transmissions between servers, and servers and clients. The encryption and decryption mechanism should be as close to the content producer and consumer as possible within the design.
N.4.1.18	Describe your solution's ability to comply with all OIT standards enclosed or identified herein, recommendations contained within National Security Agency (NSA) / Information Assurance Directorate (IAD) and/or SANS Institute publications, in that order of precedence.
N.4.1.19	Describe your solution's ability to support user roles or classifications that can be dynamically assigned at sign-on to permit users with the proper security level to authenticate at any system workstation, local or remote. Role classification should be defined by user capabilities.
N.4.1.20	Describe your solution's ability to lock user accounts that have been inactive (no sign-on activity) for a specified period of time.
N.4.1.21	Describe your solution's ability to automatically log off users that have been inactive for a specified period of time.
N.4.1.22	Describe your solution's ability to use the single-sign on security paradigm, utilizing standard mechanisms such as ADFS/SAML, LDAP, or identity management.
N.4.1.23	Describe your solution's ability to provide a process/methodology for asset classification to ensure that sensitive or confidential data is encrypted during storage and encryption.
N.4.1.24	Describe your system access control granularity: 1. By function: specific application functions, or groups of functions that may be performed; 2. By data content: specific records, or groups of records, upon which a function may perform (including View, Add, Delete, Edit, and Refresh); and 3. By location: restricted access by IP address and MAC address.
N.4.1.25	Describe how your solution allows for data mining and analysis for information security forensics in the cases of fraud or criminal investigation and to evaluate potential vulnerabilities.

2.5.1.4.2. Encryption

ID	Requirement
N.4.2.1	Describe your solution's ability to use Standard Internet encryption techniques, including the use of Secure Socket Layer (SSL), 128-bit encryption or better, TLS (Transport Layer Security), and digital certificates through recognized Certificate Authorities.
N.4.2.2	Describe your solution's ability to develop a process/methodology for asset classification to ensure that sensitive or confidential information is encrypted during storage and transmission.
N.4.2.3	Describe how sensitive data is stored in databases in encrypted form.

2.5.1.4.3. User Management and Access Control

ID	Requirement
N.4.3.1	Describe your solution's ability to utilize user authorizations or profiles to determine application access to, but not limited to the following roles: 1. "Read" access to any data; 2. "Add" access to any data; 3. "Modify" access to any data; 4. "Delete" access to any data; 5. Each function key for which access is granted; 6. Each command for which access is granted; 7. User classification or role; and 8. Production (live) or training mode.
N.4.3.2	Describe your solution's ability to comply with all OIT password policies.
N.4.3.3	Describe your solution for internal and external users IDs. IDs should be established through security administrators. Security administration functions can be deleted by function and/or user groups.
N.4.3.4	Describe how your Security administration functions can be delegated from the security administrator to an authorized user role.
N.4.3.5	Describe how both internal and external user groups' access control should be role-based. This means access to resources will be granted based on a user's function.
N.4.3.6	Describe how users can be aggregated by roles into user groups and sub-group capabilities.
N.4.3.7	Describe how user groups are defined; access can be assigned at the group level.

N.4.3.8	Describe how a user can belong to multiple groups. The solution should provide for session expiration after a user logs on to a new session.
N.4.3.9	Describe how each role access control should be performed at the following levels: 1. By function: this refers to specific application functions, or groups of functions that the user can or cannot perform; 2. By data content: the user can be restricted to access individual records, or groups of records, within an application function; and 3. By location: access control can be granted only at specified locations (e.g., through static IP addresses or MAC address).

2.5.1.4.4. Remote Access

ID	Requirement
N.4.4.1	Describe how you handle internal and external users who need to access the system remotely (e.g., department inspectors, county inspectors). For these users: 1. All accesses should be from authorized workstations that can be properly identified; 2. All data downloaded to workstations should be logged and encrypted; and 3. A process should be identified as part of the asset classification to determine if/when it may be appropriate to allow the actual download of information to a workstation/mobile device.
N.4.4.2	Describe how your solution accommodates users who need to access the system remotely for administration, operation and application support functions. Remote access will need to follow the OIT standards and policies found at http://oit.state.co.us/ois/policies

2.5.1.5. System Management and Configuration

2.5.1.5.1. Management and Administration

ID	Requirement
N.5.1.1	Describe how your solution provides for software upgrades and maintenance that do not affect the production system (no downtime) in a load-balanced environment.
N.5.1.2	Describe how your solution enables modification of a majority of the components of the system by system administrators to meet changing federal and state standards without the need to contract with a vendor to make changes. This should typically be accomplished via the use of configuration tables.
N.5.1.3	Describe how your solution provides an explanation of their service and support philosophy, how it is carried out, and how success is measured.

N.5.1.4	Describe how you maintain configuration integrity. The solution should support configuration control for all configurable elements, including auditing, rollback, roll-forward, and configuration change transactions with the ability to both import and export configurations.
N.5.1.5	Describe how your solution allows for CDPHE to modify business rules and tables based upon appropriate role-based access.
N.5.1.6	Describe how your solution provides a method to issue unique account numbers for facility owners.
N.5.1.7	Describe how your solution enables DEHS and other authorized staff to change the information on pending records when information on applications does not coincide with information on the supporting documentation.
N.5.1.8	Describe how your solution cross-references the new data entry with the existing data in the system and include edit checks to avoid duplicate data being entered into the system by comparing owner and facility data elements (e.g., name, street and city address).
N.5.1.9	Describe how your solution allows a user to enter a comment relating to a given owner, facility and/or transaction which can be available for viewing by all system users or can be restricted to only certain users.
N.5.1.10	Describe how your solution prioritizes application change request lists. All change requests should be accompanied by detailed requirements. Application enhancements and updates will be based on this list.
N.5.1.11	Describe your solution to a rigorous transfer to production process. All application software changes should be reviewed and approved by authorized personnel before placing into production libraries.
N.5.1.12	Describe your solution to the software configuration management process. All artifacts related to a software release should be organized and stored into a configuration management tool. There should be a simple process to back-out any application updates if required.

2.5.1.5.2. Application - Rules

ID	Requirement
N.5.2.1	Describe how your solution is able to associate owner records with facilities and record the ownership. Multiple facilities should be accommodated.
N.5.2.2	Describe how your solution allows for override capabilities to create a new owner record and/or change information on existing record on duplicates.
N.5.2.3	Describe how your solution links unique transaction records to the owner and/or facility that they are associated with.

N.5.2.4	Describe how your solution is owner-centric and provides the ability to support entities as well as individuals.
N.5.2.5	Describe how your solution maintains current owner ID or issue owners a unique ID. The solution should allow for storing facility alias identifiers from legacy data and adding new alias identifiers.
N.5.2.6	Describe how your solution captures owner data based on a business rules associated to owner types (e.g., individual, business).
N.5.2.7	Describe how your solution provides the ability to input and maintain investigation information and associate this information to an owner record.
N.5.2.8	Describe how your solution allows corrections of the error in the record and reporting of a corrected document, when an error is found. Version changes should be retained and not written over.
N.5.2.9	Describe how your solution provides accurate and timely information. The operational databases should be updated in real-time when business transactions occur.
N.5.2.10	Describe your solution's ability to "undo" updates so a record can be "restored" to its previous state.
N.5.2.11	Describe your solution's ability to be able to provide financial transactional records (e.g., registrations, plan reviews).
N.5.2.12	Describe how your solution provides a comprehensive and robust inquiry/search capability.

2.5.1.5.3. Business Rules Management

ID	Requirement
N.5.3.1	Describe how one single rules repository can be implemented, where DEHS business rules will be defined, updated and maintained while maintaining role based access.
N.5.3.2	Define your rules using a set of simple user interfaces. A DEHS administrator will be able to maintain the rules, without extensive training requirements.
N.5.3.3	Define your version control capabilities. A set of business rules can have multiple versions, some of which can be concurrently deployed. This is important because, in some instances, past business rules will need to be retroactively applied.
N.5.3.4	Describe your granular security authorization capabilities. Different users can be authorized to manage different rule sets.
N.5.3.5	Describe your solution's extensive reporting capabilities, including rules update history, where used, and cross references.

N.5.3.6	Describe your solution's capabilities to extensively test the business rules to ensure correctness.
N.5.3.7	Describe how your solution holds business rules in tables. Business rules should not be hard coded.

2.5.1.5.4. Business Intelligence

ID	Requirement
N.5.4.1	Describe how data extraction from the following sources are used to support business intelligence tools: 1. Owner-centric database, containing owner and facility information for all types of facilities; and 2. Work flow information, including staff assignments and work queue volumes.
N.5.4.2	Describe your solution's analysis capabilities. These include, but are not restricted to the following: 1. Query, calculating, and summarizing capabilities; 2. Ability to scan large amount of data to review trends, patterns, and correlations; and 3. Ability to display data in a visual and pictorial manner, with tabular and/or detail data prefixed by column definition.
N.5.4.3	Describe how your solution provides access to online system help files that describe fields, forms, and data requirements, as well as procedures from system documentation.
N.5.4.4	Describe how your solution provides access to an online DEHS user-guide manual that describes fields, forms, and data requirements, as well as procedures and automatic updates of the manual by DEHS administrators.
N.5.4.5	Describe how your solution provides the ability to query the DEHS manual and to allow automated updates by DEHS administration.
N.5.4.6	Describe how your solution provides interfaces to DEHS Code of Colorado Regulations (CCR), Administrative rules, memos, forms, state or field office address lists and other useful reference information as provided by the department. The Administrative role should have the ability to add, change, or delete the content.
N.5.4.7	Describe how your solution provides functionality so that all data entry fields should have "help" with explanations of the field requirements.
N.5.4.8	Describe your ability to provide a complete set of documentation describing all application components. All documents should be reviewed and approved before acceptance.

N.5.4.9	Describe how your solution is capable of supplying the DEHS IT help desk with an FAQ set for user problem resolution.
N.5.4.10	Describe how knowledge transfer & technical documentation is required of the vendor to State staff.

2.5.1.6. Database

2.5.1.6.1. Database and Data Management

ID	Requirement
N.6.1.1	Describe how your solution stores all enterprise data in relational database management system (RDBMS), which conforms to OIT standards and policies for database platforms.
N.6.1.2	Describe how your solution has the capability to execute scheduled, unattended online system database backups without affecting system performance.
N.6.1.3	Describe how your solution provides or supports the ability to restore from system database backups.
N.6.1.4	Describe how your solution provides or supports a robust system backup/archiving tools and strategies.
N.6.1.5	Describe how your solution provides a logging feature that logs entries, changes, and/or deletions to any data (data transaction recovery log).
N.6.1.6	Describe how your solution processes selected data in real time. This means that any data changes should be done while the system is online. The change should take effect immediately.
N.6.1.7	Describe how your solution includes staging, production, training, UAT, reporting, and development systems. The user's access level needs to allow the user to be able to select the system that corresponds with the desired system.
N.6.1.8	Describe how your solution supports ODBC-compliant relational database technology.
N.6.1.9	Describe how your solution provides for access to, and manipulation of, the data in the database through a standard management system.
N.6.1.10	Describe how your solution provides tools for database design and development, including documentation, data dictionary, diagramming, normalization, database generation, screen design and generation, report design and generation, and procedure maintenance tools.
N.6.1.11	Describe how your solution provides for the development and maintenance of relational database structures for the support of DEHS.
N.6.1.12	Describe your tools, methods, and processes to perform data modeling functions, resulting in the creation of conceptual, logical, and physical data models.

N.6.1.13	Describe your Metadata Directory. The directory will contain but is not limited to the following information for each data element: 1. Description of the data element; 2. Location where the data element is stored; 3. The application programs that access the data element; 4. The system of record for the data element; 5. The entity relationship diagrams for the system database; and 6. The type of actions that can occur on each data element.
N.6.1.14	Describe how your solution supports the storing of images as a separate file in the file system with pointers to the database.
N.6.1.15	Describe how your solution accurately disseminates historical data, the solution should provide for storage of the code value at the time of record data entry for code-driven fields.
N.6.1.17	Describe how your solution facilitates full Boolean searching, including phonetic indices where appropriate. The solution should provide the ability to use multiple criteria when searching for data, including archived data.
N.6.1.16	Describe how your solution depends on a relational storage engine. The solution should comply with the ANSI 1989 standards for SQL (i.e. support transaction logging with commit, rollback, and roll forward facilities for restores, referential integrity, table driven coding structures, etc.).
N.6.1.17	Describe how your solution permits Business Intelligence and Auditing systems access to the transactional data, with the minimum latency possible.
N.6.1.18	Describe how you make provisions at no additional cost, that all data can be exported upon termination of contract with full referential integrity.
N.6.1.19	Describe how your solution database should be a standalone database for State of Colorado data only (no commingling).

2.5.1.6.2. Data Backup and Recovery

ID	Requirement
N.6.2.1	Describe how all database systems have audit log files that capture before and after images.
N.6.2.2	Describe how all databases have point-in-time recovery capabilities. This means that upon any failure, the database can be recovered to the last point of consistent state.

2.5.1.7. Auditing and Reporting

2.5.1.7.1. Audits and Logging

ID	Requirement
N.7.1.1	Describe all access activities – including user, date, time, resources (Web pages, services, etc.) accessed – should be logged.
N.7.1.2	Describe how the administrator should have the ability to specify levels of logging.
N.7.1.3	Describe how all user activities should be logged and reportable. Activities include, but are not limited to the creation, modification, deletion, void, and viewing of records in the database. The log should include, but not be limited to user identification, date, time, resources (Web pages, services, etc.) accessed, and fields modified.
N.7.1.4	Describe your solution's ability to support canned and ad hoc reporting capabilities against the security logs.
N.7.1.5	Describe your solution's ability to support data mining reports providing trend/threat analysis to identity information security vulnerabilities.
N.7.1.6	Describe your solution's ability to allow for system-generated alerts on security violations.
N.7.1.7	Together with configuration management, describe your complete audit trail tracing all application changes. The audit trail should include date/time, developer, and descriptions.
N.7.1.8	Describe how your solution tracks each transaction using a unique number.
N.7.1.9	Describe your solution's ability to put a hold status on an application when an applicant is not able to supply all of the required documentation.

2.5.1.7.2. Publications/Reports

ID	Requirement
N.7.2.1	Describe your solution's ability to utilize an ad hoc reporting tool that allows trained users to create reports from data, or if not available, the solution should allow the connection of BI tools (e.g. Tableau) directly into the database or into a real-time copy of the database.
N.7.2.2	Describe your solution's ability to have a report batch monitor that controls the number of reports that may be run at a given time for each server.
N.7.2.3	Describe your solution's report scheduler that can schedule reports to be automatically run at user-defined times.
N.7.2.4	Describe how your solution supports reports, both of real-time and snapshot data that are publishable to an intranet or the Internet.

N.7.2.5	Describe how your solution provides authorized users with appropriate access to see reports on transactions started, in-process, and completed for staff in their area of responsibility by user and time parameters.
N.7.2.6	Describe how your solution provides the ability to reprint reports on demand.
N.7.2.7	Describe how your solution distributes reports by an electronic interface or allows for printing to paper.
N.7.2.8	Describe your regular, scheduled reporting such as end of day, accounting/financial, and others.
N.7.2.9	Describe your ad hoc reporting requirements, where users need to create one time reports or saved reports on an as needed basis.

2.5.1.7.3. Auditing and Reporting

ID	Requirement
N.7.3.1	Describe how your solution facilitates the above activities; there should be a standard reporting tool for all reports. This tool should be used against all data sources, for creating both scheduled and ad hoc reports, including flexibility in formats and document types (e.g., PDF, XML, csv, doc(x)).

2.5.1.8. Messaging

2.5.1.8.1. Messaging

ID	Requirement
N.8.1.1	Describe how your solution provides the ability for users to communicate externally to include Internet email, etc.
N.8.1.2	Describe how your solution provides email integration capabilities with both desktop and cloud-based mail clients (e.g. Microsoft Outlook or Gmail).
N.8.1.3	Describe how your solution provides the ability for individuals with the appropriate level of access to disseminate alert messages to a grouping of users.
N.8.1.4	Describe your solution's capabilities of providing or interfacing to a correspondence subsystem for the generation of correspondence and other documents required in the DEHS business work flow. This subsystem should be able to generate letters, documents, and other DEHS-configurable correspondence that aligns with DEHS business rules, automatically fill the configurable correspondence with the appropriate data from the system, and associate the correspondence with the owner's account.
N.8.1.5	Describe your solution's have email capabilities to support workflow-triggered correspondence to individuals and/or groups, with both content and attachments derived from system data.

2.5.1.8.2. Email

ID	Requirement
N.8.2.1	Describe your solution's capability of logging correspondences for auditing purposes. The log should include information on sender, data/time, and topics. It is desirable that the logging activities will be automated.
N.8.2.2	Describe how Emails would integrate with both desktop and cloud-based mail clients (e.g. Microsoft Outlook or Gmail).
N.8.2.3	Describe how you accommodate outbound correspondence, owner email addresses and fax numbers should be able to be stored and maintained in the customer database.

2.5.1.9. General

2.5.1.9.1. General

ID	Requirement
N.9.1.1	Describe how your solution supports electronic data access to third-party systems for query/exchange (e.g., Web services, ODBC, data warehouse/flat file, API, FTP, SFTP).
N.9.1.2	Describe how your solution defines and explains the approach to service oriented architecture.
N.9.1.3	Describe how your solution supports authentication of an electronic report/interface data source.
N.9.1.4	Describe your solution's ability to receive and respond to queries from authorized external systems and/or databases.
N.9.1.5	Describe your solution's capability for creation of outbound electronic forms that combine data from the operation database and the image database (signature image).
N.9.1.6	Describe how your solution provides a flexible set of indices that can be defined for the documents and images.
N.9.1.7	Describe how all scanned documents should be stored online for the duration that the business rules have defined as the retention period. After the retention period, documents can be archived and removed from online viewing.
N.9.1.8	Describe how a document can be moved to "off-line" storage; the document management system should retain a location indicator which will show an operator the document's current location.
N.9.1.9	Describe how your solution stores document images at a minimum resolution defined by the State or Department.

N.9.1.10	Describe how all documents within the defined retention period should be retrievable using one of the indices that are defined and entered for the document.
N.9.1.11	Describe how your solution allows only authorized users to access documents.
N.9.1.12	Describe how your solution associates documents with corresponding data records.
N.9.1.13	Describe how document images are displayed inside a browser.
N.9.1.14	Describe how document images are stored in an industry standard format (e.g., TIFF, JPEG, etc.).
N.9.1.15	Describe your solution's ability to add notations, in free text form, to a document image.
N.9.1.16	Describe how your solution accommodates different document properties. The solution should support multi-page documents, double-sided documents, and different document sizes.
N.9.1.17	Describe how authorized system users have assigned work queues. A user can examine their work queue at any time and review any outstanding assignments that will require their attention.
N.9.1.18	Describe how your solution supports the assignment of some activities as high priority – either automatically through business rules, or manually assigned by employees. High priority transactions should be highlighted within a worker's work queue and an alert (e.g., email, pop-up, text message) should be sent to them and retained with the record.
N.9.1.19	Describe how your solution has the capability to define user groups and departments. Through this definition, workloads can be distributed among employees. Supervisors within a department should have the ability to make specific assignments.
N.9.1.20	Describe how your solution has the capability to archive all data, including images, in the operational database for historical reference, at fixed intervals, based on retention dates specified by the State or Department.
N.9.1.21	Describe how archived data is verified before being purged from online storage.
N.9.1.22	Describe your solution's automated procedures in place to perform archival activities. Archival procedures should be based upon predetermined rules specified by the State or Department.
N.9.1.23	Describe how archived information and documents should be organized so that they can be accessed and retrieved efficiently & effectively.
N.9.1.24	Describe how your solution allows authorized users to override DEHS's archival schedule. When an override is put in place the user will be required to identify a reason for it and the system will create an override notification.

N.9.1.25	Describe your solution's ability for authorized users to create and modify forms. There should be an audit trail of these activities.
N.9.1.26	Describe how your solution supports version control for the forms.
N.9.1.27	Describe how your solution supports indexing and management of metadata about each form (e.g., where it draws information from or stores data to).
N.9.1.28	Describe how your solution contains a central database for forms, with functions for efficient and effective indexing, storage and retrieval of forms.
N.9.1.29	Describe how the forms are stored and displayed in standard document formats (e.g., PDF, with reasonable backward compatibility).
N.9.1.30	Describe your solution's compatibility with different document types such as form templates, including spreadsheets and word processed documents.
N.9.1.31	Describe how your solution is able to merge and integrate system data into forms for printing. The retrieved form should be merged with data from the integrated operational database and/or document image database (e.g., signatures and photos), to be incorporated as part of outbound notices/correspondences to customers.
N.9.1.32	Describe the application capabilities to use the forms as templates.
N.9.1.33	Describe how your solution works effectively with form templates, spreadsheets, and word processor documents.
N.9.1.34	Describe how you provide remote customer support through telephone, email, and the web (including 3rd party components). Details of the support should be provided with the proposal.
N.9.1.35	Describe how your solution follows Mountain Standard Time (including daylight savings changes).
N.9.1.36	Describe how you develop the solution utilizing IT best practices. The system should be tested and free of bugs at time of delivery. Any bugs detected after delivery should be fixed at vendor cost up to 90 days from delivery and should meet security best practices. Any vulnerability identified after delivery will be fixed at the vendor cost.
N.9.1.37	Describe how your solution clearly identifies responsibilities, costs, and entitlements related to minor and major upgrades, hotfixes, and patches.
N.9.1.38	Describe how you disclose the licensing and usage enforcement requirements or other restriction usage, security, and accessibility.

N.9.1.39	Describe your solution in regards to DEHS Service Level Agreement that contains agreements regarding ongoing support time frames and cost.
N.9.1.40	Describe how your solution provides configuration assistance which should be provided for an agreeable amount of time as set forth in the Service Level Agreement.
N.9.1.41	Describe how your solution provides a means for an electronic signature to be captured, saved, and associated to a specific activity as well as an individual facility.
N.9.1.42	Describe how your solution includes tools to facilitate scheduling tasks, prioritizing based on risk, enforcement follow-up, and assigning to appropriate staff based on specific variables, such as seasonality of facility operation.
N.9.1.43	Describe how your solution includes a spelling check, grammar check, auto-save, and dictionary feature that can be used with the system.

2.5.1.10. Standards

2.5.1.10.1. Standards

ID	Requirement
N.10.1.1	Describe how your solution complies with current Agency and State of Colorado technology standards and policies throughout the term of the contract.

2.5.1.11. System Implementation

2.5.1.11.1. Application Development

ID	Requirement
N.11.1.1	Describe how all requirements should be documented and captured using a common requirements development tool.
N.11.1.2	Describe how Use Cases should be developed as part of the requirements process.
N.11.1.3	Describe how your solution's standard process for change tracking, defect management, and issue monitoring.
N.11.1.4	Describe the standard process for configuration management, version control, and release management.
N.11.1.5	Describe how preference is given to a solution that has no local installation (exe file) on an end user's machine.

2.5.2. Functional Requirements

The requirements in this section pertain to the entire system and all programs. They describe the functions needed by the business. Also see the Non-Functional requirements section for additional requirements that pertain to the entire system and all programs.

2.5.2.1. Applications, Licensing and Renewals

ID	Requirement
F.2.1.1	Describe how your solution provides a means to enter facility and multiple contact information for any program.
F.2.1.2	Describe how your solution provides a means to enter a license renewal request for a facility with an active or current license. This includes updating or confirming information provided for the current license and documenting payment.
F.2.1.3	Describe how your solution provides a means to collect contact information about the individuals (owners/applicants) who submit applications. This should be stored in a way that allows the individual to be associated with multiple facilities/licenses.
F.2.1.4	Describe how your solution incorporates functions to enforce acceptable values, format, and completeness of data submitted for an application.
F.2.1.5	Describe how your solution provides a means for users to update information supplied as part of an application.
F.2.1.6	Describe how your solution provides a means to document the receipt of payment. This includes entering, at a minimum, the date, amount, and type of payment. It also involves assigning a payment status, which may impact reporting of active facilities.
F.2.1.7	Describe how your solution provides a means for the assigned inspector to indicate the steps and information that will be required to complete the licensing process for the specific facility from a menu of possible actions.
F.2.1.8	Describe how your solution provides a means for the assigned inspector to verify all required licensing steps are complete and then have the license indicated as “Approved” following review.
F.2.1.9	Describe how your solution provides a means for users to generate and print a license. This includes printing licenses individually and in a daily batch. Licenses should be laid out to print on a pre-printed license template provided by DEHS. Users should have the ability to re-print an original single license.
F.2.1.10	Describe how your solution allows for there to be multiple licenses for a single facility, and the fees should be tracked by license type.

F.2.1.11	Describe how your solution provides a means for users to generate and print notices to be mailed to facilities prior to the date they are due to renew their license, with configurable lead times. These notices should be pre-populated with applicant and business information. The renewal notices should be able to be printed individually and/or in a batch. Users should have the ability to re-print a single renewal notice in the office and in the field. The system should be able to specify a license as either on a calendar year or a fiscal year cycle.
F.2.1.12	Describe how your solution provides a means for users to document that required information was not received and a license renewal request was deemed “Incomplete.”
F.2.1.13	Describe how your solution provides a means for users to generate an incomplete renewal letter when processing an incomplete license renewal request.
F.2.1.14	Describe how your solution provides a means for users to create a facility profile including information such as the location, business name, address, ownership, water and sewer information, and contacts. The system should allow for creation of a facility without having an associated active license or license application since there are some establishments which are not licensed but may have a specific service that is subject to inspection (e.g., schools and child care centers).
F.2.1.15	Describe how your solution provides a means to capture profile information that identifies the program and type of facility that is being entered into the system. A facility should be able to have multiple programs and multiple facility types associated with it.
F.2.1.16	Describe how your solution should provide a means to associate a facility with multiple owners and maintain a history of ownership including indication of the current owner(s).
F.2.1.17	Describe how your solution maintains a history of all licenses issued for a specific location, to an owner, and to a business entity.
F.2.1.18	Describe how your solution provides a means to maintain documents required for the licensing approval process that verify compliance with federal, local, and state laws, rules, and regulations. Documentation can include PDFs or other accessible attachments that show content of written letters, wastewater permits, etc.
F.2.1.19	Describe how your solution provides a means to assign a risk category to each license that identifies the inspection frequency based on risk of activities, food products prepared or processed, and/or inspection history. Management level users should be able to reassign risk as needed.
F.2.1.20	Describe how your solution includes an indication to users when there are high risk violations associated with a facility for which an application or renewal request has been submitted. Records indicating as having non-compliance issues should also be identifiable for reports.

2.5.2.2. Inspections

ID	Requirement
F.2.2.1	Document how the solution provides a means for the users to enter data collected for routine inspections per state and federal statutes and rules and regulations specific to the type of facility. The types of inspections include, but are not limited to: 1. Retail Food Inspections (including Mobile Retail Food Inspections); 2. Manufactured Foods Inspections; 3. Shellfish Inspections; 4. Schools Inspections; 5. Child Care Inspections; 6. Dairy Plant Inspections; 7. Dairy Farm Inspections; 8. Dairy Equipment, Haulers, Samplers Inspections; and 9. Environmental Agriculture Inspections.
F.2.2.2	Document how the solution provides a means for the users to enter special inspection data and associate it to an individual facility. Inspections for a special circumstance are performed on an as-needed basis and use the same forms as routine inspections.
F.2.2.3	Document how the solution includes a means to record an inspection not associated with a licensed facility, for example an outbreak investigation that involves an unlicensed food facility.
F.2.2.4	Document how the solution provides a means to associate inspection data with a specific facility.
F.2.2.5	Document how the solution provides a means for users to generate an inspection report for completed inspections. The user should have the option to display the report on screen, print the report, or save the report as a PDF for emailing.
F.2.2.6	Document how the solution incorporates the current variety of inspection reports.
F.2.2.7	Describe your solution's ability to provide a means for the users to enter a complaint on a facility.
F.2.2.8	Describe your solution's ability to provide a means for users to track complaints and associate a complaint with an establishment when appropriate, or maintain a complaint without associating it to a facility.

F.2.2.9	Describe your solution's capability to allow users to generate a report of a completed complaint, and the user should have the option to display the report on screen, print the report, or save the report as a PDF for emailing.
F.2.2.10	Describe your solution's capability to calculate risk for designated facility types based upon formulas supplied by DEHS. Managers should have the ability to add/remove individual facilities to/from risk-based status. Managers should have the ability to manipulate the inspection due date for those facilities that are not assigned to risk-based calculations.
F.2.2.11	Describe your solution's capability to provide a means for the users to output risk scores in a delineated format for import into other systems.
F.2.2.12	Describe how the solution allows inspectors and Managers to generate a list of inspections by inspector including the date, location, type, and contact information for the facility.
F.2.2.13	Describe how the solution allows inspectors to review previous inspections, inspection reports, licensing history, laboratory reports and results, and violations associated with a facility license. This will allow verification that previous violations found during inspection are permanently corrected.
F.2.2.14	Describe how the solution provides the user with the ability to save and associate laboratory reports and results with a facility.
F.2.2.15	Describe how the solution notifies an inspector of required tasks such as an upcoming or overdue inspection. The system should also include warning messages when required information is missing.
F.2.2.16	Describe how the solution provides a means to associate a facility with an inspector. The users should be able to assign inspectors to facilities based on different levels: Program, county, city, zip code, and individual facility. Users should be able to reassign facilities on all levels as needed.
F.2.2.17	Describe how the solution allows for weighted violations and inspection scoring as defined by DEHS. These specifications should also be available in the inspection Field Client for use by inspectors in both an online and offline capability.

2.5.2.3. Billing and Payment

ID	Requirement
F.2.3.1	Describe how your solution provides a means for documenting payments and generating invoices to notify applicants that they have an amount due.
F.2.3.2	Describe how your solution provides a means for scheduling when letters will be run and printed.

F.2.3.3	Describe how your solution provides a means for users to verify the receipt of appropriate payment for a specific license(s) application that has been submitted.
F.2.3.4	Describe how your solution allows associating a payment with the specific fee it is intended to address. This includes associating the same payment with one or multiple facilities or facility types. For example, users should be able to record that the owner of multiple facilities submitted a payment specific to one facility or submitted one check to cover the license renewals for more than one facility.
F.2.3.5	Describe how your solution provides a means for users to document that insufficient funds were received when processing a license request.
F.2.3.6	Describe how your solution allows the generation of a license when the appropriate fee is paid. The system should allow a user, based on specific permissions, to change the fee status of a facility and adjust the amount of an original invoice, with audit trails, and allow a license to be generated without having to create a new invoice.
F.2.3.7	Describe how your solution provides a means for users to document that an invoice has been sent to collections.
F.2.3.8	Describe how your solution allows a user to re-print a single invoice.
F.2.3.9	Describe how your solution allows the scheduling of second, third and final late notices to the customer when required payments have not been received.

2.5.2.4. Program Administration

ID	Requirement
F.2.4.1	Describe how your solution provides the ability for authorized users to define and store user profile information, such as permissions, for administrators and other users.
F.2.4.2	Describe how your solution will be able to maintain a list of county agencies that contract work with the state and should also allow users to define and assign geographical areas to these contract county agencies.
F.2.4.3	Describe how your solution retains all changes to facility data and all historical information pertaining to name and/or ownership in addition to all inspections and extra information associated as attachments.
F.2.4.4	Describe how your solution provides a means for Managers to maintain coding systems for risk classification and types of facilities.
F.2.4.5	Describe how your solution provides a means for users to generate a distribution list for the purpose of notifying facility representatives of informational or time sensitive material via email, mail, fax, or telephone communication. Users should be able to generate lists based on variables such as type of facility or license type to target communication to a specific group or number of groups within the licensed community.

F.2.4.6	Describe how your solution supports management of compliance and enforcement actions associated with a license or operator by providing a means for tracking letters sent, closures, suspensions, civil penalties issued, condemnations, embargoes, or revocation of licenses.
F.2.4.7	Describe how your solution allows the System Administrator to assign users to multiple agencies and allowed to change these assignments as necessary.
F.2.4.8	Describe how your solution allows the recording of facility/inspection supplementary data to include, but not be limited to: broken equipment seals, voluntary food condemnation, regulation variances, milk samples, milk drug residue testing, environmental sampling, and commissaries.
F.2.4.9	Describe how your solution allows the System Administrator to assign security permissions for specific user groups. For example, one LPHA agency may have the ability to read/write data for their assigned facilities, but may only have the ability to view data for other LPHA agencies or have other LPHA agencies' data hidden from view entirely.

2.5.2.5. Data Access

ID	Requirement
F.2.5.1	Describe how your solution provides a means for users to access all data including event tracking. This may be through a data warehouse or other appropriate means. This access is in addition to standardized reports or queries generated from within the application.
F.2.5.2	Describe how your solution provides the ability for users to create standard reports, based on user permissions. Standard reports provide pre-defined data sets in a consistent format that can be requested through a report menu. These recurring reports should be produced in a manner such that they can be displayed on the screen, printed in hard copy, saved to a file, or imported into another software product. To allow for some limited customization of standard reports, the system should allow users to enter data selections or sort multiple parameters to limit the scope of data included in the report or method of presenting the data.
F.2.5.3	Describe how your solution provides the ability for users to build reports and save report templates, based on user permissions. These reports include filtering capabilities. Users should be able to enter selection parameters and query the system.
F.2.5.4	Describe how your solution provides a means to schedule when reports will be run, printed, or emailed.
F.2.5.5	Describe how your solution provides a means for users to view, print, export, and save all reports, based on the user's permissions. The reports should be able to be exported and saved in different file formats (e.g., PDF, xls(x), and doc(x)).
F.2.5.6	Describe how your solution provides a means for Managers to build and save report templates with filtering abilities.

F.2.5.7	Describe how your solution provides a means for the administrator role to customize dashboards per user; customize fields on the user interface, to include facility pages and inspection pages; and customize content displayed in fields.

2.5.2.6. Foodborne Illness/Outbreak Response and Food Recall

ID	Requirement
F.2.6.1	Describe how your solution provides a means for users to track data associated with a foodborne illness and/or outbreak.
F.2.6.2	Describe how your solution provides a means to associate the record of a foodborne illness/outbreak event to other foodborne illness/outbreak event records and to a facility, and it should have the ability to be updated with multiple dated entries. The system should be able to associate a foodborne illness/outbreak event to a complaint.
F.2.6.3	Describe how your solution provides a means for users to record embargoed goods, including the ability to track the goods for notification purposes to any/all facilities.
F.2.6.4	Describe how your solution provides a means for users to track data associated with a food product recall.
F.2.6.5	Describe how your solution provides a means to associate a record of a food product recall event to other food product recall event records and to a facility, and it should have the ability to be updated with multiple dated entries. The system should be able to associate a food product recall event to a complaint.

2.5.2.7. Public Access

ID	Requirement
F.2.7.1	Describe how your solution allows a public user to conduct and view limited searches of facility inspections via a website. The preferred method of data publication is via REST-based web services.
F.2.7.2	Describe how your solution allows an internal user to redact restricted information on a facility inspection before it is viewed by the public.
F.2.7.3	Describe how your solution complies with all OIT standards and policies pertaining to external access to any CDPHE application.
F.2.7.4	Describe how your solution allows a facility owner to login to a portal in order to view and update their facility information; apply for a new license/permit; view inspections conducted on their facility; receive notification of renewal fees due; receive notification of past-due fees; pay fees and print a license on-demand;
F.2.7.5	Describe how your solution integrates with our CORE financial system through specifications directed by the State Internet Portal Authority through the use of APIs.

2.5.2.8. Complaint Investigations

ID	Requirement
F.2.8.1	Describe how your solution allows facility and owner information to be entered so that an inspector can investigate if the facility is required to be regulated. This facility and owner information should not reside in the database tables that house actively regulated facilities (i.e. the main facility and owner tables); however the system should have the tools to convert a prospective facility to an active facility if the facility is required to be regulated. This screen should have data entry capabilities to record the prospect investigation process.
F.2.8.2	Describe how all inspections and additional information transfer with the prospective facility when it becomes an active facility.

2.6. DETAILED DEFINITION OF WORK

This solicitation seeks to ensure that the resulting Contract supports the State's needs and to achieve the best combination of quality, service, price, and any other key components outlined below:

2.6.1. Business Requirements

Offeror must detail how the Proposal complies with the requirements above.

Offeror's Response:

Q 2.5.1	

2.6.2. Technical Requirements

Offeror must detail how the Proposal complies with the requirements above.

Offeror's Response:

Q 2.5.2	

2.6.3. Management Requirements

Offeror must detail how the Proposal complies with the requirements above.

Offeror's Response:

Q 2.5.3	

2.6.4. Security Requirements

The Proposal should clearly state, with no exception, agreement to comply with, and to ensure personnel doing work for the State under any contract resulting from this RFP will comply with, the State of Colorado Information Security Policies (CISP) promulgated by the Colorado Chief Information Security Officer and available at http://oit.state.co.us/ois/policies. The Proposal Should clearly state that the Proposal Should be in compliance with the current OIT Technology Standards promulgated by the OIT Chief Technology Officer and available at http://www.oit.state.co.us/cto/ea/standards. The Proposal should clearly state agreement to complete the assigned vendor portions of the System Security Plan as directed by the Office of Information Security and as reflected in Attachment C - System Security Plan Template.

a. To the extent applicable to the Proposal, Offeror agrees that the Price Proposal includes all costs and expenses for the security requirements stated below. Any additional costs to add security controls or to verify the security controls described below will be the obligation of the Awarded Offeror, and any addition or change to the Price Proposal will be disallowed.

b. For each category of security control listed below, describe how the Proposal will comply, or briefly explain why the control would be inapplicable.

i. Role-based access control (RBAC) for any logical interactive access to applications and/or supporting systems (e.g., user-interface, maintenance);
ii. Auditable logs/trails for successful and attempted access to the application/system, administrative actions such as add/delete/modify user permissions, and/or other auditable events;
iii. Business continuity and disaster recovery planning, including defined recovery time and recovery point objectives;
iv. Third-party certification or audit results that fully covers the scope of the work included in the Proposal, such as a SOC 2 Type II report, FISMA compliance certification, or similar information security assurance certification, or agreement to allow the performance of security audit and penetration tests as requested by OIS or its designee;
v. Documentation of an industry-standard secure system development lifecycle (S-SDLC), including written policies and procedures, documented results of vulnerability scans and/or penetration testing, evidence of and/or plans for remediation of known vulnerabilities, etc.;
vi. Infrastructure hardening consistent with all standards published on CISecurity.org, or similar;
vii. Any additional policy, procedure, practice, or evidence not described above related to compliance with the Colorado Information Security Policies or the NIST Cybersecurity Framework on which the CISPs are based?

c. Will the solution(s) described in the Proposal require any exceptions from compliance with the CISPs or other information security controls described above?

Offeror must detail how the Proposal complies with the requirements above. Offeror must be prepared to provide evidence in connection with any aspect of this answer upon request by the State.

Offeror's Response:

Q 2.5.4	

2.6.5. Accessibility

The Proposal Should clearly state agreement to comply with **Section 508 of the U.S. Rehabilitation Act of 1973, as amended, and** with the most current version of the Web Content Accessibility Guidelines (WCAG) available at https://www.w3.org/TR/WCAG21/. To the extent applicable to the Proposal, Offeror agrees that the Price Proposal includes all costs and expenses associated with compliance with these

accessibility requirements. Any additional costs to add accessibility features will be the obligation of the Awarded Offeror, and any addition or change to the Price Proposal will be disallowed.

Describe how the Proposal will comply with these accessibility requirements, or briefly explain why any requirement would be inapplicable. Will the solution(s) described in the Proposal require any exceptions from compliance with these requirements?

Offeror's Response:

Q 2.5.5	

2.6.6.Key Personnel

Offeror must detail the key personnel to be assigned to this project.

Offeror's Response:

Q 2.5.6	

2.6.7. Performance Measures

Offeror must detail the key performance measures on which the project would be evaluated.

Offeror's Response:

Q 2.5.7	

2.7. REFERENCES AND EXPERIENCE

The State reserves the right to use Colorado State Agencies and other state governments as references. In addition to these references, Offerors must include the following with their Proposal:

1. Provide three references, including contact name, individual titles, locations, and a current telephone number. The references provided should be associated with work completed corresponding to the nature of the work in scope and size called for in this RFP and Statement of Work.

2. Provide written documentation of two years' experience in managing and technically performing similar projects for at least three entities of similar size and complexity with similar statements of work and related requirements. Include State or company name, point of contact, location, phone number, and brief project description along with the outcome of the project.

List your references and similar experiences using the text box below:

Q 2.6	

2.8. PRICE PROPOSAL

Offeror should submit its Price Proposal with the required data in the same format as Attachment B price sheet.

Offeror must describe the market resources, methodology, and technology used to determine the proposed rates. ONLY ATTACHMENT B WILL BE CONSIDERED TO CONTAIN THE PRICE TERMS OF OFFEROR'S PROPOSAL.

Information provided in response to Question 2.7 above is to assist in evaluating the reasonableness of Offeror's Price Proposal. Any additional costs, fees, or charges listed in Question 2.7 will be disallowed under any contract resulting from this RFP.

Q 2.7	

2.9. PRE-PERFORMANCE MEETING

Upon execution of a contract, CDPHE should conduct a review of the contract requirements with key personnel of the State and an Awarded Offeror. The purpose of the meeting is for all working parties to gain a better knowledge of contract requirements, to ask and answer questions, and to conduct a needs assessment so that the transition to work performance will commence on a smooth and timely basis.

2.10. PRIME – SUBCONTRACTOR RELATIONSHIPS

Any Offeror who proposes to contract with any third-party entity or individual to provide the goods or services described in the Proposal Should agree to be the Prime Contractor with the State and to subcontract with any such third party. The Proposal should identify any known third party that will perform as a subcontractor. The State will only enter a contract with the Prime Contractor. The State will require that the Prime Contractor ensure subcontractor compliance with the terms of the RFP and any resulting contract. The Prime Contractor should direct the work and deliverables of any subcontractor and should coordinate any subcontractor activities. Any contract between the Prime Contractor and any subcontractor should comply with all applicable Federal and state laws and should provide that such subcontract be governed by the laws of the State of Colorado, and that venue for any disputes should be in the City and County of Denver, Colorado.

2.11. PERFORMANCE OUTSIDE THE UNITED STATES

Any Offeror who proposes to perform any aspect of the work outside the United States, or to contract with any third-party to perform any aspect of the work outside the United States, Should identify in its proposal the work to be performed outside the United States and the reason why it is necessary or advantageous to perform such Services outside the United States. To the extent that performing any work outside the United States will have an impact on the price of the work or any other aspect of the Proposal, the Offeror must provide information sufficient for the State to evaluate the costs and benefits of performing the same work within the United States. The State, in its sole discretion, may elect to approve or deny any request to perform work outside the United States. Failure to include information sufficient to allow the State to

approve or deny any such request should be grounds for the state to reject any Proposal or to decline to award a contract to the Offeror.

Any work performed outside the United States should be subject to the same terms of this RFP and any contract, including but not limited to terms relating to personnel security and background checks, information security, and subcontracting. An Offeror proposing to perform any work outside the United States should provide information regarding the Offeror's ability to comply with such provisions for work performed at any non-US location.

2.12. EXECUTIVE GOVERNANCE COMMITTEE (EGC)

The Awarded Offeror should be required to comply with the State's Executive Governance Committee (EGC) project gating methodology and plan for all EGC gating items to be included as part of the overall project plan. As part of the EGC gating process, the Awarded Offeror will be required to cooperate with a third-party Independent Verification & Validation (IV&V) vendor engaged by the State to provide IV&V services related to the project. More information can be found in the Project Lifecycle Methodology & Governance policy, available at http://www.oit.state.co.us/about/policies.

SECTION 3: RESPONSE FORMAT

3.1. SIGNED REQUEST FOR PROPOSALS (RFP) SIGNATURE PAGE.

Offeror must submit a signed Request for Proposal Signature Page to be considered for this award. The State may, at the State's sole discretion, accept an alternative signed document by a person legally authorized to bind the Offeror to the Proposal. If an alternative to the Signature Page is accepted, the Offeror Should submit a signed Request for Proposal Signature Page within one business day of notice of such acceptance.

3.2. PROPOSAL SUBMISSION

Proposals must be received on or before the Proposal Submission Deadline as indicated on VSS and on the Schedule of Activities in this RFP. **Late proposals will not be accepted.** It is the responsibility of the Offeror to ensure that its Proposal is received by the CDPHE Procurement and Vendor Services Office on or before the Proposal Submission Deadline. Offerors mailing their proposals should allow sufficient mail delivery time to ensure receipt of their proposals by the Deadline. All proposals submitted must be delivered sealed within a package, envelope, box, or other container.

> Proposals must be submitted in a sealed package with an appropriate label affixed. The label must show the following information:
>
> Offeror's Name
> RFP-No.
> Proposal Due Date and Time
>
> Offeror must separate its Price Proposal from the other elements of the Proposal.

A Request for Proposals Signature Page (Attachment A) has been provided. The Proposal must be signed in ink, preferably blue ink, by an officer of the Offeror who is legally authorized to bind the Offeror to the Proposal. Proposals that are determined to be at a variance with this requirement may not be accepted.

3.3. REQUIRED COPIES

Offerors are required to submit one (1) original copy and the required number of paper copies as stated on the Request for Proposal Signature Page. Offerors are also required to submit an electronic copy of the entire proposal in PDF and Microsoft Excel format.

.

3.4. OFFEROR FINANCIALS

The State reserves the right to request that each Offeror provide a copy of its most recent certified and audited financial statements. The State reserves the right to review such financial documentation for all Offerors or only for Awarded Offerors as a method of determining financial responsibility.

3.5. CONTENT QUALITY

Do not include extensive artwork, unusual printing or binding, or other materials that do not enhance the utility or clarity of the Proposal. General statements without supporting documentation are not encouraged. All submitted documents should be printed double-sided on recycled paper, and in a format that is easy to copy or scan, e.g. without attached binding material, clips, etc. Paper should be light colored, preferably white, and dark backgrounds should not be used. If system screenshots or other images are included, images should be of sufficient quality to ensure readability of all elements displayed.

3.6. PROPOSAL ORGANIZATION

The original hard-copy Proposal should be submitted in a 3-ring binder with all material clearly labeled in a manner that will facilitate the committee members' evaluation. Information that is responsive to each specific question or requirement of this RFP should be labeled to facilitate review and evaluation. The State reserves the right to consider any required information as non-responsive if each response in the Proposal is not clearly labeled with the appropriate section number of the RFP.

Please **segregate** the Price Proposal in the original response, all required copies, and any electronic submission, as applicable.

3.7. EXCEPTIONS TO THE RFP OR THE MODEL CONTRACT LANGUAGE

Any exception or objection to the requirements of this RFP must be clearly stated within the Proposal by reference to the corresponding section of the RFP. Failure of a Proposal to comply with all requirements of this RFP may be grounds for denying an award to the Offeror.

The Proposal should include a list of any proposed changes to the Model Contract language or a statement confirming that no changes are being proposed. Proposed changes to the Model Contract must be presented as proposed alternative or substitute language that would be acceptable to the Offeror. Any objection to Model Contract language presented without an alternative should be deemed a rejection of that language, and may be grounds for denying an award to the Offeror.

SECTION 4: PROPOSAL EVALUATION

An Evaluation Committee will judge the merit of Proposals received in accordance with the criteria outlined in this section. CDPHE will undertake an intensive, thorough, complete, and fair evaluation process. All Offerors should be afforded fair and equal treatment throughout the evaluation process. The sole objective of the Evaluation Committee will be to evaluate and compare the Proposals so that the Committee can recommend for award the Proposal determined to be most advantageous to the State of Colorado.

4.1. BASIS FOR AWARD

The requirements stated within this RFP represent the minimum performance requirements necessary for response as well as desired elements of performance. All Proposals must meet the mandatory minimum requirements established by this RFP to be eligible for award.

For proposals that are considered susceptible to award, evaluation will be based on price as well as the following factors:

Mandatory Minimum Requirements- Pass /Fail
Non-Functional Requirements
Functional Requirements
Business Requirements
Security Requirements
Price Proposal

Supplementary information that may be requested by the Evaluation Committee, such as clarifications, presentations, or the non-cost aspects of "Best and Final" offers, may be incorporated into the Committee's evaluation of the factors stated above, or may be evaluated and considered as separate evaluation factors. If considered separately, any supplementary information will be considered by application of the same evaluation factors stated above.

4.2. EVALUATION PROCESS

The information in this subsection is intended to provide Offerors with a general outline of the evaluation process. The process described herein is a description of a typical process that the State may use to evaluate Proposals submitted in response this RFP. The State reserves the right to modify or adapt the procedures described herein to the extent permitted by law and by the Colorado Procurement Code. To the extent permitted by law, no party should be aggrieved by any deviation from the process described herein.

At any point during the evaluation process, the Evaluation Committee may, within its reasonable discretion, determine that any Proposal is not susceptible of award under this RFP. Such a determination may be based on a Proposal's failure to meet any mandatory or otherwise material requirement of this RFP. To the extent permitted by law, no party should be aggrieved by any decision of the Evaluation Committee to remove a

Proposal from consideration on the basis of any reasonable perception of the Proposal's insufficiency to meet the requirements of this RFP or to be in the best interest of the State.

4.2.1. Evaluation Based On Initial Proposals

Each Evaluation Committee member will independently evaluate the merits of Proposals received in accordance with the evaluation factors stated within this RFP, followed by discussion of the entire Evaluation Committee. The State reserves the right to make an award(s) on receipt of initial Proposals, so Offerors are encouraged to submit their most favorable Proposal at the time established for receipt of Proposals.

4.2.2. Competitive Range

The State may establish a competitive range of Offerors whose Proposals have been initially evaluated as most responsive to the requirements and reasonably susceptible of being selected for award.

4.2.3. Clarifications/Discussions

The CDPHE Purchasing Agent may conduct discussions with Offerors for the purpose of promoting understanding of CDPHE's requirements and the Offeror's Proposal, clarifying requirements, and making adjustments in services to be performed and in prices and or rates. Offerors engaged in such discussions may be sent a list of questions and will be given a specified number of days in which to formulate and submit written responses to the questions and provide any related revisions to their initial Proposals. The nature of the questions will generally be for the purpose of clarification and related revisions to Proposals are generally permitted in response. Such revisions will be at the option of the Offeror, but will be limited to the guidelines set forth in CDPHE's requested clarifications. No major changes will be permitted, nor will CDPHE accept any additional written materials not relevant to the questions/clarifications requested. Clarifications/discussions may be limited to Offerors within the Competitive Range.

4.2.4. Presentations/Demonstrations

Offerors may be given an opportunity to provide an oral presentation or demonstration in Phase II only. CDPHE Purchasing Agent reserves the right to select the site. During the presentation, an Offeror should provide specific responses to the questions posed to it and may also make a summary presentation of its Proposal. The presentation should include a description of how Offeror's revisions, if any, may have affected the overall nature of its offer as compared to the initial Proposal. The presentation is typically limited to 60 minutes, but may be longer if the Evaluation Committee deems it necessary. If the Evaluation Committee members believe it to be necessary, a question/answer period may follow. Presentations/Demonstrations may be limited to Offerors within the Competitive Range.

4.2.5. Best and Final Offers (BAFO)

Adjustments may also be allowed in conjunction with clarifications, discussions, presentations, and/or demonstrations, but only to the extent such revisions are consistent within the Proposal requirements. These revisions will be considered as Best and Final offers. Such adjustments must be submitted in writing.

4.2.6. Final Evaluations

If the Evaluation Committee did not make a recommendation based on initial proposals, the Committee will re-evaluate all Proposals considered susceptible of award together with any supplementary information gained from clarifications, presentations, or BAFOs. Final evaluation may be completed independently by each Committee member, or may be completed through a collaborative discussion of the Committee. The goal of Final Evaluation Should be to arrive at a recommendation. The Committee's approval of a Decision Memo, as further described below, should be the documentation of the result of the Committee's final evaluations.

4.2.7. Award Recommendations

Upon completion of the evaluation process, the Evaluation Committee will formulate a recommendation as to any Proposal that is determined to be most advantageous to the State within available resources. The Committee will draft and agree to a Decision Memo, explaining the Committee's evaluation of the proposals submitted and the basis for its recommendation. The Decision Memo will be forwarded to the CDPHE Procurement and Contracts Unit Director for review and approval.

4.3. NOTICE OF INTENT TO AWARD

If the recommendation in the Decision Memo is approved by the CDPHE Procurement and Contracts Unit Director, a Notice of Intent to Award will be published on Colorado VSS. Upon posting of the Notice, all non-confidential and non-withdrawn documents submitted by all Offerors in connection with this RFP should become public records and will be available for public inspection upon request. Any Awarded Offeror will be contacted by CDPHE to complete post-award requirements.