State of Colorado

Department of State

Statewide Electronic Pollbook System

RFP #: CDOS-EPOLL-1

Request For Proposals

Document 1 of 3

November 12, 2013

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

The Colorado Department of State (CDOS) is issuing this Request for Proposal (RFP) to purchase software for the implementation of a Statewide Electronic Pollbook System in order to meet the requirements of House Bill 13-1303, also known as the Voter Access and Modernized Elections Act (VAMEA).

Elections Environment in Colorado

The VAMEA legislation has changed the Colorado elections environment in major areas including registration requirements and voting model.

Registration Requirements

Before the VAMEA legislation, there was a 30 day registration deadline which limited the amount of registration activity performed during voting activity. Now, there is no registration deadline allowing any eligible resident to register new, update their registration, vote by mail, or vote in person up to 7pm on Election Day.

Voting Models

Before the VAMEA legislation, elections were conducted using one of three available voting models; Polling Place, Vote Center, or Mail Ballot. Each County had the authority to select the model best suited to their jurisdiction with Mail Ballot prohibited for major elections. After the VAMEA legislation, elections must be conducted using a Voter Service and Polling Center voting model.

Polling Place Model

In a Polling Place model voters must go to their assigned Precinct Polling location to vote in person on Election Day. Early Voting is available at any designated Early Voting location to any voter in the County for 2 weeks before Election Day. Early Voting ends the Friday before the election. A voter may request a Mail-In ballot to be returned and counted subject to a signature verification process. Mail-In ballot requesters are not eligible to vote in person on Election Day.

Vote Center Model

In a Vote Center model voters may go to any designated Vote Center location in the County to vote in person on Election Day. All Vote Center locations in the County must use a shared Electronic Pollbook on Election Day. Early Voting is available at any designated Early Voting location to any voter in the County for 2 weeks before Election Day. Early Voting ends the Friday before the election. A voter may request a Mail-In ballot to be returned and counted subject to a signature verification process. Mail-In ballot requesters are not eligible to vote in person on Election Day.

Mail Ballot Model

In a Mail Ballot model all Active eligible voters are sent a Mail Ballot with sufficient time to receive, vote and return prior to 7pm on Election Day. Inactive voters may activate their registration and receive a Mail Ballot either in person or before a deadline for mailing ballots. All Mail Ballots are counted subject to a signature verification process.

Provisions for in person voting on Direct Record Electronic (DRE) voting machines exist to accommodate disabled voters.

Voter Service and Polling Center Model

In a Voter Service and Polling Center (VSPC) model all Active eligible voters are sent a Mail Ballot with sufficient time to receive, vote and return prior to 7pm on Election Day. VSPC locations are opened a minimum of 8 days before and including Election Day. Any eligible resident of the County including unregistered individuals and voters that were already sent a Mail Ballot may appear at any VSPC to do any of the following:

- Register as a voter
- Update their address
- Update their registered name
- Unaffiliated voters may affiliate with a political party
- Cast a ballot
- Receive a Mail Ballot
- Receive a replacement Mail Ballot
- Return a Mail Ballot
- Cast a Provisional ballot

1.1 Entities

Along with the CDOS, all 64 Colorado counties are required to comply with the VAMEA legislation. The County Clerks in each of the 64 Colorado counties are responsible for administering elections. As a result, the Clerk's offices will be direct beneficiaries of the statewide system.

1.2 Scope of the Statewide Electronic Pollbook System

The scope of this project is to install a fully tested and proven solution for the implementation of a statewide electronic pollbook system that fully complies with all applicable federal and state laws and the business requirements of CDOS and counties.

In general, the system will:

- Protect the voter information of all registered citizens
- Maintain the integrity of the electoral process
- Enable county election officials to administer efficient, fair, and impartial elections
- Provide an audit capability; and
- Establish stronger coordination inherent in a statewide system

1.3 Project Schedule and Location

The estimated schedule for project activities in shown in Section 2.5. It is the goal of the CDOS to implement the electronic pollbook system for use during the 2014 Primary Election in June 2014, with a “code complete” target date of April 25, 2014.

CDOS requires the project vendor to obtain their own office space for the project needs.

Meetings with State officials that are associated with the project will be at CDOS offices.

1.3.1 Vendor Access

The Vendor will have access to

- CDOS Elections staff
- CDOS Operational Support Team
- CDOS Chief Information Officer (CIO)
- Documentation of information systems; and
- Any documentation that exists relating to the applicable systems, including State agency policies, procedures and business processes.

The Vendor will be required to execute CDOS End-User Computing Policy and CDOS Privacy Agreement. (Appendices A & B).

SECTION 2: ADMINISTRATIVE INFORMATION

2.1 Issuing Office

This RFP is issued by the CDOS. The CDOS is the sole point of contact concerning this RFP.

To the extent possible, the CDOS intends to follow all state procurement rules and statutes applicable to RFPs. However, the CDOS is headed by the Secretary of State, who is not subject to such rules and statutes pursuant to section 24-2-102 (4), Colorado Revised Statutes (C.R.S.). To the extent that there is any inconsistency between this RFP process (including the RFP itself) and any state procurement rule or statute, it shall be conclusively presumed that the Secretary of State has elected not to follow such rule or statute.

2.2 Official Means of Communication

During the solicitation process for this RFP, **all** official communication from the CDOS to Vendors will be via postings on the Colorado BIDS System website (www.bidscolorado.com). The CDOS will post notices that will include, but are not limited to, modifications to administrative or performance requirements, answers to inquiries received, clarifications to requirements, and the announcement of the apparent winning Vendor. **It is the sole responsibility of Vendors to monitor the Colorado BIDS System website carefully and regularly for any such postings.**

2.3 Statement of Purpose

This RFP provides prospective Vendors with sufficient information to enable them to prepare and submit proposals for consideration by CDOS to achieve the goals of this RFP.

2.4 Scope of RFP

This RFP contains instructions governing the proposal to be submitted and identifies material to be included therein; sets forth mandatory requirements that must be met for the Vendor to be eligible for consideration; and specifies other optional requirements to be met by each Vendor.

2.5 Schedule of Activities

Activity	Date
RFP posted on Colorado BIDS System website	November 12, 2013
Prospective Vendors Written Inquiry Deadline (No Questions Accepted After This Date and Time)	November 18, 2013 3:00 PM (Mountain Time)
Answers to inquires posted	November 22, 2013
Proposal Submission Deadline	December 12, 2013 3:00 PM (Mountain Time)

Activity	Date
Oral Presentations	December 17 – December 20, 2013
Award Announced (Estimated)	December 23, 2013
Estimated Project Start Date	January 6, 2014
Project Deployment Date	April 25, 2014
Contract Duration (4 months Development, 2 statewide elections After Release On-Site Support)	January 2014 through November 2014
Optional 2-year Maintenance Agreement	December 2014 through November 2016

2.6 Inquiries

Vendors may send mail, e-mail, or fax inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the Schedule of Activities. Send all mail inquiries to:

Department of State
Attn: Trent Parker, CDOS-EPOLL-1 -- Inquiry
1700 Broadway, Suite 200
Denver, Colorado 80290

Address fax inquiries to: Attention: Trent Parker, fax (303) 869-4878. Address e-mail inquiries to Trent.Parker@sos.state.co.us.

The only "official" response to a Vendor's inquiry is a response that is published as a modification on the Colorado BIDS System website (www.bidscolorado.com). Vendors should not rely on any other statement that alters any specification or other term or condition of this RFP.

2.7 Modification or Withdrawal of Proposals

Proposals may be modified or withdrawn by the Vendor prior to the established due date and time.

2.8 Proposal Submission

Proposals must be received on or before the date and time indicated in the Schedule of Activities. Late proposals will not be accepted. It is the responsibility of the Vendor to ensure that the CDOS receives the proposal on or before the proposal submission deadline date and time. Vendors mailing their proposals shall allow sufficient mail delivery time to ensure receipt of their proposals by the deadline specified. The proposal package shall be delivered or sent by mail to:

Department of State
Attn: Trent Parker
CDOS-EPOLL-1
1700 Broadway, Suite 200
Denver, Colorado 80290

The State of Colorado Request For Proposal Cover Page is found with this RFP material on the Colorado BIDS System website. The cover page MUST be signed in ink by an officer of the Vendor legally authorized to bind the Vendor to the proposal. The officer must also clearly print his or her name on the cover page and date it. The signed cover page is to be included with the proposal copy that is marked ORIGINAL.

Proposals, that are determined to be at a variance with this requirement, may not be accepted.

Faxed or emailed proposals will not be accepted.

Proposals must be submitted in a sealed package. The outer envelope of the package must show the following information:

<VENDOR'S NAME>
RFP NUMBER: CDOS- EPOLL-1
<PROPOSAL DUE DATE AND TIME>

The CDOS desires and encourages proposals to be submitted on recycled paper, printed on both sides. While the appearance of proposals and professional presentation is important, the use of non-recyclable or non-recycled glossy paper is discouraged.

2.9 Addendum or Supplement to Request for Proposals:

The CDOS reserves the right to make changes to this RFP, its attachments, and appendices. Such changes will be implemented through the posting on the Colorado BIDS System website (www.bidscolorado.com) of an addendum (or addenda) to this RFP. It is Vendors' responsibility to monitor the Colorado BIDS System website for changes to this solicitation.

2.10 Oral Presentations and Demonstrations

Vendors may be asked to make oral presentations and/or demonstrations. Such presentations will be at the Vendor's expense. The State will be conducting an Architecture Assessment Validation (AAV) on the vendor's proposed architecture during the Oral preparation period. The State expects complete cooperation with the AAV vendor during that period.

2.11 Acceptance of RFP Terms

A proposal submitted in response to this RFP shall constitute a binding offer. The autographic signature of an officer of the Vendor legally authorized to execute contractual obligations shall indicate acknowledgment of this condition. A submission in response to this RFP acknowledges acceptance by the Vendor of all terms and

conditions including compensation, as set forth herein. A Vendor shall identify clearly and thoroughly any variations between its proposal and the CDOS's RFP. Failure to do so shall be deemed a waiver of any rights to subsequently modify the terms of performance, except as outlined or specified in the RFP.

2.12 Confidentiality and Open Records

CDOS is subject to Colorado Open Records laws (24-72-101 through 24-72-112, C.R.S.). Thus, documents and other materials received by CDOS and its employees may be subject to public disclosure.

Upon receiving an official open records request, CDOS will immediately notify the applicant and, as needed, seek legal guidance for a ruling on confidential information. Applicants should be aware that CDOS can only respond to requests to review records to the extent that such information is contained in CDOS's files.

CDOS will deny the right of inspection of records containing trade secrets, privileged information, and confidential commercial and financial data. Applicants should clearly mark areas of the application they consider to be trade secrets, privileged information, and confidential commercial and financial data. The entire application may not be marked "confidential". Please note that information considered confidential at the time of application may cease to be so at a later date.

2.13 Confidential / Proprietary Information

Any restrictions of the use or inspection of material contained within the proposal shall be clearly stated in the proposal itself. Written requests for confidentiality shall be submitted by the Vendor with the proposal. The Vendor must state specifically what elements of the proposal are to be considered confidential/proprietary.

Confidential or proprietary information must be readily identified, marked and separated from the rest of the proposal. Co-mingling of confidential or proprietary information and other information is NOT acceptable. Neither a proposal, in its entirety, nor proposal price information will be considered confidential and proprietary. Any information that will be included in any resulting contract cannot be considered confidential.

The CDOS or Attorney General will make a written determination as to the apparent validity of any written request for confidentiality. In the event the CDOS does not concur with the Vendor's request for confidentiality, the written determination will be sent to the Vendor. If the request is denied, Vendor will have the opportunity to withdraw its entire proposal, or remove the confidential or proprietary restrictions. *See* Section 24-72-200.1 *et seq*., C.R.S., as amended, the Colorado Open Records Act ("CORA").

2.14 RFP Response Material Ownership

All material submitted regarding this RFP becomes the property of the CDOS. Proposals may be reviewed by any person after the "Notice of Intent to Make an Award" letter has been issued, subject to the terms of the Colorado Open Records Act, section 24-72-201 et seq., C.R.S.

2.15 Agreement Type

The services provided and work performed pursuant to this RFP shall be performed on a firm, fixed-price, and turnkey basis in accordance with the terms of a negotiated contract with the selected vendor. The CDOS shall not be obligated for any other payments to Vendor except as approved in writing by the Secretary of State, or designee, of CDOS and the State Controller, or designee. The parties may agree to changes during the course of performance, within the scope of the original procurement, through the use of change orders, contract amendments or contract modifications.

"Turnkey" means that Vendor shall deliver the system to the CDOS, which shall be consistent with the system performance specifications and shall be comprised of all components integrated, tested, and certified for immediate use in supporting an electronic pollbook system consistent with both applicable state and federal laws and the requirements of this RFP.

2.16 Proposal Prices

Estimated proposal prices are not acceptable. Proposal prices will be considered to be your best and final offer, unless otherwise stated in the RFP. The proposal price will be considered in determining the apparent successful Vendor. All prices offered shall be FOB Destination and shall include all costs of shipping, handling, installation, training, and full system documentation and all goods and services covered by this RFP, and such other expenses as are included elsewhere in this RFP and the Vendor's proposal.

All proposed prices shall be binding until a contract is executed containing the agreed terms and prices.

2.17 Subcontractors

Vendors shall clearly explain planned use of subcontractors in their proposal, including terms of any subcontract, capabilities, experience and portion of the work to be performed by the sub-contractors. The Vendor, as prime contractor, shall be responsible for contract performance whether or not subcontractors are used. The winning Vendor will be the sole point of CDOS contact with regard to contractual matters including the performance of services and the payment of any and all charges. Current employees of the Department of State and current employees of consultant affiliates engaged in pre-existing contractual obligations as key personnel to the Department of State may not participate as resources for subcontractors of the Vendor.

Due to security concerns, no element of this RFP and resulting contract can be completed in whole or part outside of the United States of America. No information or direct reference of this RFP and resulting contract can be sent, distributed, or referenced in whole or part outside of the United States of America. The CDOS will NOT accept any variance or modification of this term and condition.

2.18 Bid Clarification / Vendor Guarantee

All information contained in this RFP and its appendices, including amendments and modifications thereto, reflect the best and most accurate information available to the

CDOS at the time of RFP preparation. Inaccuracies in such data will not constitute a basis for change in the payments to the contractor nor a basis for a legal recovery of damages, either actual, consequential or punitive except to the extent that such inaccuracies are the result of intentional misrepresentation by the CDOS.

It is the responsibility of the Vendor to review and understand all information, instructions, specifications, and terms and conditions in this RFP. All Vendors, by submitting a signed bid, guarantee to the CDOS that they understand and agree to the terms and conditions of this RFP and that they will not default from performance by virtue of a mistake or misunderstanding. Vendors shall seek clarification from the CDOS of any information, instruction, specifications, terms and/or conditions, which they determine to be unclear. The failure of a Vendor to seek clarification shall be deemed a waiver of any such clarification.

2.19 Bid Opening

As soon as is practical after the proposal submission deadline date and time, at the location noted for bid submission, the bids shall be opened and a register shall be prepared of the bids submitted in response to this solicitation. The following information will be read and entered into the bid register: name of Vendor and delivery date. The bid register will be available via the Colorado BIDS System website (www.bidscolorado.com).

2.20 Selection of Proposal

An Evaluation Committee will review and score offers submitted to determine which offer is the most advantageous to the CDOS and the State of Colorado. The CDOS will notify all Vendors via a posting on the Colorado BIDS System website (www.bidscolorado.com) of the results of the RFP evaluation. The posting will be an announcement of "Notice of Intent to Make an Award" which will name the apparent successful Vendor.

2.21 Award of Contract

The award will be made to the Vendor whose proposal, conforming to this RFP, will be the most advantageous to the CDOS and the State of Colorado, based on several criteria, including but not limited to price. A contract must be completed and signed by all parties concerned. In the event the parties are unable to enter into a contract, the CDOS may elect to cancel the "Notice of Intent to Make an Award" letter and make the award to the next most responsive Vendor.

2.22 Acceptance of Proposal Content

The contents of the proposal (including persons specified to implement the project) of the successful Vendor will become contractual obligations if acquisition action ensues. Failure of the successful Vendor to accept these obligations in a State contract, purchase order, or similar authorized acquisition document may result in cancellation of the award and such Vendor may be removed from future solicitations.

2.23 RFP Cancellation

The CDOS reserves the right to cancel this entire RFP or individual components at any time, without penalty.

2.24 Incurring Costs

The CDOS is not liable for any cost incurred by Vendors prior to issuance of a legally executed contract, purchase order, or other authorized acquisition document. No property interest, of any nature, shall occur until a contract is awarded and signed by all concerned parties.

2.25 Non-Discrimination

The Vendor shall comply with all applicable State and federal laws, rules, and regulations prohibiting unfair employment practices and discrimination on the basis of race, color, religion, national origin, age or sex.

2.26 Rejection of Proposal

The CDOS reserves the right to reject any and all proposals, waive informalities and minor irregularities in proposals received, and to accept any portion of a proposal or all items proposed if deemed in the best interest of the CDOS and State of Colorado. Failure of a Vendor to provide any information requested in this RFP may result in disqualification of the proposal.

2.27 Parent Company

If a Vendor is owned or controlled by a parent company, the Vendor must provide the name, main office address, and parent company's tax identification number in the proposal. The Vendor responding to the RFP must provide its tax identification number.

2.28 Press Releases

Press releases, release of information, or any communications with media entities pertaining to this RFP must NOT be made prior to execution of the contract without prior written approval by CDOS.

2.29 Contract Cancellation

The CDOS reserves the right to cancel, for cause, any contract resulting from this RFP by providing timely written notice to the contractor.

2.30 Certification of Independent Price

2.30.1 Certification

By submission of a proposal each Vendor 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 this 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 Vendor or with any competitor;

(b) Unless otherwise required by law, the prices which have been quoted in this proposal have not been knowingly disclosed by the Vendor and will not knowingly be disclosed by the Vendor prior to bid opening, directly or indirectly to any other Vendor or to any competitor; and

(c) No attempt has been made or will be made by the Vendor to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

2.30.2 Individual Certification

Each person signing the Colorado Request for Proposal Cover Sheet of this proposal certifies that:

(a) He/She is the person in the Vendor's organization responsible within that organization for the decision as to the prices being offered herein and that he/she has not participated, and will not participate, in any action contrary to 2.29.1(a) through 2.29.1(c) above; or

(b) He/She is not the person in the Vendor's organization responsible within that organization for the decision as to the prices being offered herein but that he/she has been authorized in writing to act as agent for the persons responsible for such decision in certifying that such persons have not participated, and will not participate, in any action contrary to 2.29.1(a) through 2.29.1(c) above, and as their agent does hereby so certify; and he/she has not participated, and will not participate, in any action contrary to 2.29.1(a) through 2.29.1(c) above.

2.30.3 Proposal Not Considered For Award Conditions

A proposal will not be considered for award where 2.29.1(a), 2.29.1(c), or 2.29.2 above has been deleted or modified. Where 2.29.1(b) above has been deleted or modified, the proposal will not be considered for award unless: (1) the Vendor furnishes with the proposal a signed Statement which sets forth in detail the circumstances of the disclosure and (2) the head of the agency, or his designee, determines that such disclosure was not made for the purpose of restricting competition.

2.31 Taxes

The State of Colorado, as 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 sales taxes in accordance with section 39-26-704(1), C.R.S. The CDOS State and Local Sales Tax Exemption Number is 98-02565. Vendor is hereby notified that when materials are purchased in certain political sub-divisions (e.g., the City & County of Denver), the Vendor may be required to pay sales tax even

though the ultimate product or service is provided to the State of Colorado. This sales tax will not be reimbursed by the State.

2.32 Assignment and Delegation

Except for assignment of antitrust claims, neither party to any resulting contract may assign or delegate any portion of the agreement without the prior written consent of the other party.

2.33 Availability of Funds

Financial obligations of the State payable after the current fiscal year are contingent upon funds for that purpose being appropriated, budgeted or otherwise made available. In the event funds are not appropriated, any resulting contract may become null and void, without penalty to the CDOS.

2.34 Insurance

2.34.1 Insurance Coverage

The contractor shall procure, at its own expense, and maintain for the duration of the contract, the following insurance coverage:

- Standard Workers' Compensation and Employer Liability as required by State statute, including occupational disease, covering all employees on or off the work site, acting within the course and scope of their employment.
- Commercial General Liability Insurance written on ISO occurrence form CG 00 01 10/93 or equivalent, covering premises operations, fire damage, independent contractors, products and completed operations, blanket contractual liability, personal injury, and advertising liability with minimum limits as follows:

  a) $1,000,000 each occurrence;

  b) $1,000,000 general aggregate;

  c) $1,000,000 products and completed operations aggregate; and

  d) $50,000 any one fire.

  If any aggregate limit is reduced below $1,000,000 because of claims made or paid, the contractor shall immediately obtain additional insurance to restore the full aggregate limit and furnish to the State a certificate or other document satisfactory to the State showing compliance with this provision.
- Commercial Automobile Liability Insurance covering any auto (including owned, hired and non-owned autos) with a minimum limit as follows: $1,000,000 each accident combined single limit.
- Other Insurance - Vendor shall provide such other insurance as may be required by law, or in a specific solicitation.

2.34.2 Public and Non-Public Entities

1. **Public Entities:** If Contractor is a "public entity" within the meaning of the Colorado Governmental Immunity Act, CRS §24-10-101, et seq., as amended (the "GIA"), then Contractor shall maintain at all times during the term of this Contract such liability insurance, by commercial policy or self-insurance, as is necessary to meet its liabilities under the GIA. Contractor shall show proof of such insurance satisfactory to the State, if requested by the State. Contractor shall require each contract with a Subcontractor that is a public entity, to include the insurance requirements necessary to meet such Subcontractor's liabilities under the GIA.
2. **Non-Public Entities:** If Contractor is not a "public entity" within the meaning of the GIA, Contractor shall obtain and maintain during the term of this Contract insurance coverage and policies meeting the same requirements set forth in §13(B) with respect to Subcontractors that are not "public entities".

2.34.3 Additional Insured

The State of Colorado shall be named as additional insured on the Commercial General Liability and Automobile Liability Insurance policies. The State of Colorado shall be issued certificates as an additional insured. Coverage required of the contract will be primary over any insurance or self-insurance program carried by the State of Colorado.

2.34.4 Cancellation Prevention

The insurance shall include a provision preventing **cancellation** without 60 calendar days prior written notice to the CDOS by U.S. certified mail.

2.34.5 Insurance Documentation

Vendor shall provide the following documentation to the CDOS within 7 working days of a request, unless otherwise provided:

1. **Certificate/s** of adequate insurance coverage, each with a reference to the State being named as an additional insured, or

2. **Certificate/s** of adequate insurance coverage and an **endorsement/s** of additional insured coverage.

2.35 Independent Contractor Clause

All personal service contracts must contain the following clause:

> THE CONTRACTOR SHALL PERFORM ITS DUTIES HEREUNDER AS AN INDEPENDENT CONTRACTOR AND NOT AS AN EMPLOYEE. NEITHER THE CONTRACTOR NOR ANY AGENT OR EMPLOYEE OF THE CONTRACTOR SHALL BE OR SHALL BE DEEMED TO BE AN AGENT OR EMPLOYEE OF THE STATE.

CONTRACTOR SHALL PAY WHEN DUE ALL REQUIRED EMPLOYMENT TAXES AND INCOME TAX WITHHOLDING, SHALL PROVIDE AND KEEP IN FORCE WORKER'S COMPENSATION (AND SHOW PROOF OF SUCH INSURANCE) AND UNEMPLOYMENT COMPENSATION INSURANCE IN THE AMOUNTS REQUIRED BY LAW, AND SHALL BE SOLELY RESPONSIBLE FOR THE ACTS OF THE CONTRACTOR, ITS EMPLOYEES AND AGENTS.

2.36 Venue

The laws of the State of Colorado, U.S.A., shall govern in connection with the formation, performance and the legal enforcement of any resulting contract. Further, Title 24, C.R.S., as amended, Article 101 through 112, and Rules adopted to implement the statutes govern this procurement, except as noted in section 2.1 above. Vendor agrees that venue for any action related to performance of the resulting contract shall be in the City and County of Denver, Colorado.

2.37 Contract

Except as modified herein, the Model Personal Services Contract available at the website of the Colorado Office of the State Controller (http://coloradoc2.prod.acquia-sites.com/osc/contractgrant-forms) shall govern this procurement and is hereby incorporated by reference.

Legislative Changes

The State reserves the right to amend the contract in response to legislative changes.

Order of Precedence

In the event of any conflict or inconsistency between terms of this RFP and Vendor's proposal, such conflict or inconsistency shall be resolved by giving effect to documents in the following order: Colorado Special Provisions, contract, exhibits, RFP, and Vendor's response.

Statewide Contract Management System ("CMS")

For all contracts resulting from this solicitation, Vendor agrees to be governed, and to abide, by the provisions of §24-102-205, §24-102-206, §24-103-601, §24-103.5-101 and §24-105-102 C.R.S. concerning the monitoring of vendor performance on State contracts and inclusion of contract performance information in a statewide contract management system.

VENDOR PROPOSED TERMS AND CONDITIONS

Except as specified in Vendor's proposal, the submission of Vendor's proposal will indicate its acceptance of the terms and conditions of this RFP. Vendor must disclose in its proposal, terms and conditions or required clarifications of terms and conditions consistent with these instructions. 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.

OWNERSHIP OF CONTRACT PRODUCTS

All products produced in response to the contract resulting from this RFP will be the sole property of the State. Any exceptions must be outlined in Vendor's proposal in detail. Exceptions may serve as cause for rejection of the proposal.

2.38 Special Provisions

2.38.1 Controller's Approval

The contract shall not be deemed valid unless and until the State Controller or his designee has approved it. This section is applicable to any contract involving the payment of money by the State. However, the Secretary of State may elect, in accordance with section 2.1 of this RFP and section 24-2-102 (4), C.R.S., to execute the contract without State Controller approval.

2.38.2 Indemnification

To the extent authorized by law, the contractor shall indemnify, save, and hold harmless the State, its employees, and its agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by the contractor, or the contractor's employees, agents, subcontractors, or assignees pursuant to the terms of the contract.

2.38.3 General

(a) The laws of the State of Colorado and rules and regulations issued pursuant thereto shall be applied in the interpretation, execution, and enforcement of this contract. Any provision of this contract whether or not incorporated herein by reference which provides for arbitration by an extra-judicial body or person or which is otherwise in conflict with said laws, rules, and regulations will be considered null and void. Nothing contained in any provision incorporated herein by reference which purports to negate this or any other special provision in whole or in part shall be valid or enforceable or available in any action at law whether by way of complaint, defense, or otherwise. Any provision rendered null and void by the operation of this provision will not invalidate the remainder of this contract to the extent that the contract is capable of execution.

(b) At all times during the performance of this contract, the Contractor shall strictly adhere to all applicable federal and State laws, rules, and regulations that have been or may hereafter be established.

(c) Pursuant to section 24-30-202.4, C.R.S., the State Controller may withhold debts owed to State agencies under the vendor offset intercept system for: (1) unpaid child support debt arrearages; (2) unpaid balance of tax, accrued interest, or other charges specified in Article 22, Title 39, C.R.S.; (3) unpaid loans due to the student loan division of the department of higher education; (4) owed amounts required to be paid to the unemployment compensation fund; and (5) other unpaid debts owing to the State or any agency thereof, the amount of which is found to be owing as a result of final agency determination or reduced to judgment as certified by the Controller.

(d) The signatories aver that they are familiar with section 18-8-301 et seq., C.R.S. (Bribery and Corrupt Influences) and 18-8-401 et seq., C.R.S., (Abuse of Public Office), and that no violation of such provisions is present.

(e) The signatories aver that, to their knowledge, no State employee has any personal or beneficial interest whatsoever in the service or property described herein.

SECTION 3: CURRENT ENVIRONMENT

3.1 SCORE Current Environment

SCORE is hosted at two off-site Data Centers. Data is replicated between sites to support user loads and facilitate disaster recovery. The SCORE environment is composed of:

- Secure and Environmentally Controlled Data Center
- Microsoft/Intel Servers
- Oracle Databases
- .Net

County users access SCORE through a Citrix connection performing the following functions:

- Process voter registration applications
- Configure elections
- Issue Mail ballots
- Receive and validate Mail ballots
- Issue Early Voting ballots

On Election Day, counties capture in person voting activity on a pollbook.

Counties conducting a Polling Place election may use a paper or electronic pollbook. Electronic pollbooks at Polling Places use information exported from SCORE and do not have direct access to SCORE on Election Day.

Counties conducting Vote Center elections may use the SCORE web based Vote Center application or choose to use another electronic pollbook system. Vote Centers using the SCORE electronic pollbook have direct access to SCORE including real-time updates to registration information and voting activity. Vote Centers using another system do not have direct access to SCORE on Election Day except through a full service station which has a SCORE Citrix connection and their electronic pollbook system.

It is not required by CDOS that the proposed system be architected on the same platforms. This information is provided for informational purposes only.

SECTION 4: STATEMENT OF WORK

4.1 CDOS Review of Deliverables

The CDOS's review time will begin upon receipt of the Vendor deliverables. Review dates and times for subsequent project deliverables shall be set when the Project Plan is approved. In order to expedite the final review of each deliverable, the Vendor shall provide interim draft deliverables for preliminary review, as agreed upon with CDOS.

4.2 Deliverable Sign Off

The Vendor will accomplish the work and present the deliverables described in this section. Each deliverable must be formally accepted by CDOS before sign-off. The Vendor is responsible for scheduling acceptance "walk-through" sessions to present each deliverable to the CDOS. The following individuals (or designees) will accept or reject the deliverables:

- CDOS CIO
- SCORE Manager
- SCORE Technical Manager

Unless otherwise specified, CDOS will sign-off on the deliverable, or provide a report documenting why the deliverable is not acceptable within 10 business days (close of business) of the delivery date.

4.3 Requirements Tracking

The Vendor shall propose and utilize tools to completely document and track requirements from identification to implementation. The solution shall be a single uniform electronic method to ensure that all requirements are tracked, traceable, and testable through the project lifecycle (Requirements clarification, design, testing, and long term maintenance). The Vendor is responsible during the course of performance for identifying the requirements that they deem satisfied by project phase, software module, and date of delivery.

The selected Vendor will be responsible for providing documentation that relates Colorado's requirements as indicated in the RFP directly to the functional descriptions of the Vendor's system, and indicating how application testing is and would be performed to determine satisfaction of the requirements.

4.4 Change Tracking

The Vendor is responsible for tracking changes, regardless of whether they are initiated by the Vendor or by CDOS. All change tracking documents shall be retained, including those that CDOS does not approve. The change shall be initiated by a request that provides details of the change. The change request shall include time and dollar estimates prepared by the Vendor. CDOS must evaluate all change requests for approval or disapproval. The Vendor is responsible for timely upgrades of the existing documentation so that documentation reflects all approved changes.

4.5 Change Request Costs

Typically, the development costs can increase because of a "change request." CDOS expects to have some change requests that could result in a cost decrease as well as those that cause increases. If functionalities are excluded from the requirements, the CDOS team will submit a change request form that should result in a decrease in project cost, CDOS may use any cost decreases to offset costs resulting from other change requests.

Colorado law mandates that the Secretary of State maintain SCORE and requirements are subject to changes mandated by legislative action. This RFP's documented requirements are based upon what is known at the time this RFP is issued. CDOS may submit future change requests due to subsequent legislative changes. However, at the time of RFP delivery, the proposed solution must satisfy applicable laws.

4.6 Personnel Availability

The Vendor shall be an integral and vital member of the project and is expected to provide ongoing technical advice and to consult on project management decision- making and planning efforts. The Vendor must make their lead Project Manager available by telephone during Mountain Time (MT) business hours. Vendor must respond to a CDOS inquiry within one business day.

In addition, in the event that the State contracts an Independent Verification and Validation (IV&V), the Vendor shall make personnel, plans, lists, and other relevant documents available.

4.7 Office Equipment and Software / Deliverable Formats

The Vendor shall provide its own computer hardware and software during this project. Software to be used by the Vendor for communications and deliverables during this engagement shall be Microsoft Office and Microsoft Project, unless otherwise agreed to by CDOS. Copies of all working documents, deliverables, communications, etc. must be provided to CDOS in both hardcopy and electronic format.

4.8 Planning Requirements

The Vendor shall create a detailed Project Plan within 30 business days, unless otherwise specified, of execution of the contract in conjunction with CDOS.

In addition, the following plans will be provided on an agreeable schedule during the project.

- Project Schedule
- Change Control Plan
- Configuration Management Plan
- Conversion Plan
- Disaster Recovery / Business Continuity Plan
- Help Desk Plan
- Implementation Plan

- Issue Management Plan
- Maintenance Plan
- Organizational Change Management Plan
- Performance Test Plan
- System Availability Plan
- Risk Management Plan
- Security Plan
- Staffing Plan
- System Test Plan
    - Unit/Module testing
    - Network/Communication testing
    - Performance testing
    - Load Testing
    - Full Integration testing
    - System Acceptance testing
    - User Acceptance testing
    - Security testing
- Training Plan

The Project Schedule must be maintained in a version of Microsoft Project (as coordinated with the CDOS) and include activities, tasks, resources, schedules for conducting the analysis, design, development, testing and implementation of the Statewide Electronic Pollbook system.

The Project Schedule must include separate tasks for each activity and milestone; logical sequence and interdependencies, including those with CDOS and contractor tasks; resource requirements and assignments; target completion dates for each task and deliverable; and identification of and compliance with deadlines and milestones.

The Vendor shall develop proposed alternatives for the implementation of this project, and make a recommendation regarding the alternative the Vendor feels best suits the environment and timeframe at CDOS.

Throughout the life of the project, the Vendor shall update their Project Plan, as needed, to address changing project situations. Any changes shall be submitted, in writing, to the CDOS for written approval before any activity regarding proposed changes. The Vendor shall provide updated versions of the Project Plan in written weekly status reports to CDOS.

For each proposed change to the Project Plan, the Vendor shall assess whether any new hazards or risks are introduced into the project. The Vendor shall report if tasks need to be repeated as a result of changes to the Project Plan.

4.9 Project Monitoring Requirements

4.9.1 Monitor Execution of the Project Plan

The Vendor shall utilize metrics and other indicators of the project's progress towards its goals and monitor the execution of the project plan. Metrics shall include: project progress relative to budget/time/resources expended/projected.

4.9.2 Early Identification of Problems

The Vendor shall be responsible for early identification and communication of problems, project issues, and risks associated with execution of the Project. The primary areas of ongoing focus shall include, but not be limited to: adherence to schedule (time) and reasonableness of staffing assumptions (people).

The Vendor is responsible for tracking and managing these problems, issues and risks.

The Vendor shall proactively identify risks to the project, make recommendations to prevent and/or reduce risks, identify causes of any missed deadlines, and monitor status of corrective actions/risk intervention strategies. The Vendor shall independently conduct periodic external environmental scans to determine how changes in the external environment may impact the Project. These changes may include, but are not limited to, changes in federal and state rules, regulations, laws, budget changes, and State budget impacts.

4.9.3 Monitor Technical Compliance

The Vendor shall develop and carry out a methodology to evaluate technical aspects of the project including, but not limited to, IT systems, policies and procedures, and training. The Vendor must also monitor technical change such as new versions of software, error detection and corrections, and movement of modules into production. Vendor shall notify CDOS of any issues resulting from this activity.

4.9.4 Report Status

The Vendor shall prepare project status reports that summarize key information related to the status and health of the project. Status reporting meetings will be held weekly. The Vendor shall provide a weekly status report that contains, but not limited to, the following information:

- Executive summary on technical, business, and schedule aspects
- Progress (actual vs. planned)
- Accomplishments
- Schedules
- Risks
- Issues and Concerns
- Staffing.

The Vendor shall review project milestones and deliverables and report both positive features of the work completed as well as areas of technical or business risk.

4.10 Proposed Project Plan

The proposal must include an initial project plan based on the project phases described below. Include a description of the project approach that will be used, and the project procedures to be performed. This initial plan should include, at a minimum:

- A synopsis of how each task and the deliverables of the project's phases will be addressed.
- The responsibilities of all staff assigned to the engagement, according to each major phase and task of the project plan.
- A description of the methodology used to develop the Vendor's internal performance standards, the processes and tools used to monitor and measure performance against the standards, and the management reporting systems that capture this data.
- A description of the Vendor's proposed quality assurance processes and show on the schedule when internal quality assurance review tasks will produce documentation for assessment by the CDOS project team.
- A preliminary project schedule indicating milestones and estimated delivery dates for all deliverables. Vendors' proposals may comment on the phases, tasks, and deliverables to suggest optimization strategies to improve the quality of the deliverables and the timeliness of their delivery.
- A brief conceptual description of how the system will be built, and how it will operate once complete.

The CDOS has identified 6 phases to help frame the project tasks. In order to allow creativity in developing solutions, Vendors may propose alternative phases that will best meet the project needs and goals.

Phase Number	Activities
Phase 1	Planning Analysis Assessment Existing Requirements Analysis and Completion Architecture Design Disaster Recovery Design
Phase 2	Application Design Interface Design Development Software Modification Unit Testing
Phase 3	Implementation strategy System Testing

Phase Number	Activities
Phase 4	User Acceptance Testing Performance/Load/Stress Testing Security Testing Production Installation
Phase 5	Help Desk Implementation/Training
Phase 6	Final Documentation Transition to Maintenance and Support Disaster Recovery Testing

4.11 Change Control Plan

Change control is an on-going effort that affects all phases of the project. All Change Requests shall be documented. All changes to the system must be reflected in the documentation. As modifications are made that affect the original documentation (requirements, process decomposition, business rules, data flow, manuals), that documentation shall be upgraded to reflect what has actually been delivered.

The Vendor must create a change control plan and design a change request form that includes:

- A description of the change.
- Control numbering.
- Priority.
- Date submitted.
- Date Completed.
- Proposed cost of the change.
- Estimated impact on the project schedule.
- Impact on application if change is made.
- Impact on application if change is not made.
- Approval line for vendor Project Manager
- Approval line for CDOS Project Owner
- Approval line for CDOS Project Manager
- Approval line for Department of State CIO

4.12 Hardware/Operating Software

The software the Vendor creates shall run in an environment not be less than one version behind the current release at the time of purchase. CDOS will be listed as the owner of all licenses.

4.13 Data Ownership

The CDOS will be the sole owner of the data that resides in the system. No technical characteristic of the system supplied by the Vendor shall prohibit or unreasonably inhibit access to all data in all tables and files in the system provided to the CDOS pursuant to this RFP.

4.14 Security

The following are security requirement for the development of code for the Secretary of State's office:

- Proper logging of application errors, logins, failed logins and application actions. Logs should be in a standard consistent format that can be parsed easily with regex expressions.
- Password requirements:
  - Complex passwords - Must contain three out of the four following items: an upper case letter, lower case letter, number and symbol.
  - Minimum password length of 8 characters.
  - Password expiration every 90 days. Expiration should be configurable.
  - Password History with at least 24 values. Value should be configurable.
  - Accounts should be locked out after 6 incorrect login attempts. This number should be configurable.
- All developers should be trained in secure coding best practices with an emphasis on the OWASP top 10 and SANS Securing Web Application Technologies (SWAT) checklists. It would be preferred for all developers complete the SANS Securing the Developer training.
- Application should be designed to function entirely over SSL (443).
- All code should be written with system and network security requirements in mind.
- E-mail Alerts
  - May require a CAPTCHA confirmation.
  - E-mails should contain an un-subscribe link.
- Web applications must go through web penetration testing before a production release.
- All code should go through a secure code review by a qualified developer before release.
- Logon warning banners for all users that login should be present and easily changeable by a CDOS Admin**.**
- Password resets:
  - The application should allow for password resets.
  - Users should be identified before a password reset takes place by a CDOS admin.
- The application should meet the State of Colorado's Cyber Security requirements. (http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408771)
- All source code developed solely for this project must be the property of CDOS.
- The application or backend systems should disable inactive user accounts after a configurable period of time. Usually this is set to 90 days.
- Sessions which are idle for greater than 15 minutes should be required to re-authenticate.

4.15 Acceptance Test

The vendor shall propose a detailed acceptance test plan for review, modification and approval by CDOS. However, CDOS is responsible for the Acceptance Test activities. The Vendor must be available to support (i.e. conversion, restore database, run the transactions and any reports required, correct any problems discovered by the test) this acceptance test effort.

The state with assistance from the Vendor, will prepare test scripts that include the expected results. If the test is unsuccessful, it will be documented and reported to the vendor Project Manager for correction. If test results cause changes to be made to the system, appropriate regression testing must be performed to ensure that no inadvertent changes are made.

In addition to acceptance tests, CDOS may perform a mock election on the system sometime after release and before the second statewide election after release. The Vendor must be available to support up to two consecutive weeks of mock election activities.

The Vendor is responsible for the tracking and solving of problems reported for all test phases and activities.

4.16 Escrow of Source Code

Within thirty (30) calendar days after execution of the contract in conjunction with CDOS, the contractor shall deposit the source code for the software, DLLs, compilers, Data Base Schema, triggers, Data Base embedded software, firmware and any special utilities prepared by the Vendor, including all software documentation, relevant commentary, and explanations (Escrowed Material) into an escrow repository. The Vendor warrants that the source code deposited, and all subsequent deposits under this Agreement, shall include comments and documentation and will be complete and capable of compilation by a knowledgeable technician of the CDOS into an operable version. The Escrowed Material shall be maintained in good working order, sequence and business-like fashion.

Not later than every six (6) months thereafter or upon request of CDOS, the Vendor shall deposit, with a mutually agreed upon Escrow Agent (which may be the CDOS), all revisions, corrections, changes, modifications, and enhancements made to the Escrowed Material. Within seven (7) days after such deposit with the Escrow Agent, both the Vendor and the Escrow Agent shall give written notice of receipt to the CDOS. The Escrow Agent, for a period not to exceed fifteen (15) years, will retain all previous versions of Escrowed Materials.

The cost of using the Escrow Agent may be borne by the CDOS or the Vendor.

The Vendor's proposal for this escrow procedure shall contain a warranty that the Escrowed Material does not contain any expiry key or other mechanism for establishing a date or time beyond which the software license will be invalid or beyond which the software will not function properly.

Upon written notice to the Vendor and the Escrow Agent, CDOS may conduct tests of the Escrowed Material, under the Vendor's supervision, to confirm the conditions and usability of the Escrowed Material. Any direct costs associated with testing the Escrowed Materials shall be borne by the CDOS. Any deficiencies shall be corrected within 30 calendar days and all associated correction and re-test costs shall be borne by the vendor.

A default by the Vendor shall be deemed to have occurred under this Escrow Agreement upon occurrence of any of the following:

1. If the Vendor has availed itself of, or been subjected to by any third party, a proceeding in bankruptcy in which the contractor is the named debtor; an assignment by the Vendor for the benefit of its creditors; the appointment of a receiver for the Vendor; or any other proceeding involving insolvency or the protection of, or from, creditors and same has not been discharged or terminated without any prejudice to the CDOS rights or interest under this License agreement within thirty (30) days; or
2. If the Vendor has ceased its on-going business operations, or the sale, licensing, maintenance, or support of the Software to the documented requirement of this Agreement; or
3. If the Vendor offers an upgrade or release of the Software that the CDOS documents does not meet Colorado's management, operational, or legal requirements.
4. If the Vendor breaches or defaults any term or condition of the contract.

4.17 Documentation

For all documentation to be provided to CDOS under the contract, the Vendor shall first provide a draft document. With CDOS approval, the Vendor shall then prepare the final document, which must include one (1) original and one (1) softcopy file. CDOS shall have a minimum of ten (10) working days, unless otherwise agreed upon, to review and approve each draft and final document.

Documentation must be provided for the users that will explain how the application works. This documentation must be written in layman terms and clearly explains how to use the system for daily, weekly, quarterly, annual and special processing. The documentation must explain those variables that can be updated by the users.

4.18 Training

There are various areas that require training. At a minimum, the Vendor must provide the following training.

Application Training

Prior to implementation of the Statewide Electronic Pollbook System project, the Vendor shall train designated CDOS staff and selected representatives from County staff. Vendor shall ensure that the trainees understand the application and can properly use the application in a good and workman like fashion to the satisfaction of the State.

Architecture Training

Training must be conducted for up to six (6) CDOS staff members regarding the operation, maintenance, security, performance, remote management and on-site support.

Software Training

Training must be conducted for up to six (6) CDOS staff members regarding the software (excluding the application) used to support and supplement the application.

Database Training

Training must be conducted for up to four (4) CDOS staff members regarding the support and maintenance of the database.

Maintenance, Support and Operations

Training must be conducted for up to four (4) CDOS staff members on the maintenance and support of the application.

4.19 Implementation

The Vendor will be responsible for all implementation activities.

4.20 Information Technology Standards

The proposed system must comply with the State of Colorado Information Technology Standards and Rules developed or amended by the Governor's Office of Innovation and Technology (OIT) and/or as adopted by the Colorado Commission on Information Management (IMC). This information is available at: www.oit.state.co.us/

4.21 Hosting & Operational Support

Depending on the availability of additional funding CDOS may enter into a two-year Maintenance Agreement with the Vendor, who will provide operational support during that period. CDOS anticipates transitioning the operational support to CDOS staff over the two-year period.

4.22 On-Site Support

Vendor staff dedicated to this project shall operate and provide On-site Support during the first two statewide elections after release. Vendor staff must have the historical knowledge of the project, skills, expertise and capability of addressing and resolving any production problem related to the implementation. Vendor shall provide operations and maintenance support to repair any malfunction.

4.23 Application Warranty

At the end of the On-site Support period, the term of the Warranty shall commence. This will cover any problems that are discovered, after final acceptance.

If CDOS reports a suspected warranty problem, it will be evaluated to determine if it is covered by the warranty. The warranty will cover any application problem that does not

function as described by the most up-to-date copy of the requirements document, including all change requests.

4.24 Service Level Agreement

The awarded Vendor must enter into a Service Level Agreement (SLA) with the CDOS. This agreement will address various areas of service expectations such as response time, quality, accuracy and scalability.

The CDOS defines response time as the maximum time period that will elapse between the initial CDOS request acknowledgement and commencement of resolution.

The response time to a support request to the Vendor is governed by the Priority Level of the request as determined by the CDOS.

Priority Level	Description
Severe	Critical functionality failure exists with excessive risk to the ability of counties and/or other stakeholders to use the system. System or application catastrophic failure has occurred or is very likely to occur imminently.
High	Desired functionality is not as indicated in requirement. There is a high risk that the application will not perform critical functions. The issue stops counties and/or stakeholders from performing a function. No work-around is available.
Medium	Desired functionality is missing, or the application misses CDOS's expectations for delivering the functionality. Temporary work-around is available. Some risk exists. May be inconvenient for a period of time not to exceed two weeks.
Low	Desired functionality is missing, or the application misses expectations for delivering the functionality. Work-around is available. No risk exists. The matter is a cosmetic problem.

The response to this RFP should contain Service Levels common to existing and prior SLAs the Vendor has entered into for similar systems. CDOS is interested in all levels typical for systems of this kind including but not limited to application availability and system response time.

The SLA shall include four (4) levels of onsite and telephone software support at the central server locations hosting the system for 7 X 24 coverage with varying levels of response time depending upon the level of priority established by the CDOS, the registration deadlines defined in VAMEA, and VSPC hours of operation.

The SLA shall contain a description of the escalation procedure that the vendor will follow to handle support calls and assure a timely resolution of support and maintenance requests, satisfactory to the CDOS.

4.25 Billing Procedures

The Vendor shall provide an invoice no later than the 30th of the month following the month worked for all work that has been accepted and approved by the CDOS.

4.26 Payment Method

Payment shall be made after the completion of each milestone (defined by the Payment Schedule), the acceptance of the deliverables by CDOS and receipt of an acceptable invoice from the Vendor. The following individuals (or designees) must accept the deliverables before the payment will be authorized:

- CDOS CIO
- SCORE Manager
- SCORE Technical Manager

Payment for each deliverable will be based on the following estimated percentages of the total offered price excluding actual costs for any software. The CDOS shall withhold twenty percent (20%) of each payment (except for software).

Portions of the 20% holdback will be paid to the Vendor upon completion of two (2) separate milestones:

1. All deliverables have been accepted by CDOS.
2. The expiration of ninety calendar days after release of the system to CDOS.

The following table references the phased plan in section 4.10 to illustrate the distribution of payments during the course of the project.

Payment Schedule		
Phase	**Initial Payment Percentage**	**Net Payment Percentage**
Software (excluding the application)	Full cost	Full cost
Phase 1	5% (less 20%)	4%
Phase 2	10% (less 20%)	8%
Phase 3	10% (less 20%)	8%
Phase 4	15% (less 20%)	12%
Phase 5	30% (less 20%)	24%
Phase 6	30% (less 20%)	24%
Retained until 90 calendar days after release of the system.		20%
TOTAL	80%	100%

4.27 Performance Penalties and Rewards

All deliverables and performance measures in this RFP will be monitored by CDOS. Notwithstanding any conflicting terms and conditions, any and all performance issues (including untimely performance, failure to provide deliverables, etc.) must be resolved or corrected to the satisfaction of CDOS before payments will be made. CDOS reserves the right to determine if withholding of payment is warranted.

4.28 Property Rights and Ownership

Vendor shall provide to CDOS all software, research, reports, studies, data, photographs, negatives or other documents, drawings, models, materials, or work product of any type, including drafts, source code, and intellectual property (IP) prepared in the performance of the Vendor's obligations.

This work product shall be the exclusive property of the State of Colorado and the Vendor shall deliver all work product to CDOS upon completion or termination of the contract. The State of Colorado's exclusive rights in the work product includes, but is not limited to, the right to copy, publish, display, transfer, and prepare derivative works.

SECTION 5: VENDOR'S RESPONSE FORMAT

Each proposal must consist of three (3) sealed packages:

(1) The first package must be labeled “Business Proposal” and must contain one (1) original hardcopy (marked as such), fifteen (15) additional hardcopies and one (1) electronic copy (in MS Word/Excel, on CD or USB format) of the Business Proposal including the State of Colorado Request for Proposal Cover Page and a Transmittal Letter.

(2) The second package must be labeled “Cost Proposal” and must contain one (1) original hardcopy (marked as such), fifteen (15) additional hardcopies, and one (1) electronic copy (in MS Excel, on CD or USB format) of the Cost Proposal. The hardcopy documents shall be provided in 3-ring binders.

(3) The third package must be labeled “Confidential Materials” and must contain one (1) original hardcopy (marked as such), fifteen (15) additional hardcopies, and one (1) electronic copy (in MS Excel, on CD or USB format) of confidential materials submitted as part of the proposal. The hardcopy documents shall be provided in 3-ring binders. Materials in this package should contain only information provided in response to sections “Sample Project Materials” in Section 5.5.7, “Financial Information” in Section 5.5.11, and “Design, Performance and Testing Materials” in Section 5.7.

Materials contained in the third package will be destroyed or returned, at the Vendor’s option, at the conclusion of our proposal evaluation. Please include a letter indicating your preference of destruction or return of materials in the “Confidential Materials” package.

Overly elaborate proposals are not desired.

5.1 Page Limits

The CDOS may elect not to evaluate proposals that exceed the page limits specified for each required proposal section. A page is defined as one (1) side of an 8 ½” by 11” piece of paper. Font size for all narrative descriptions must be no smaller than 12 point Arial font. Margins (all sides) may not be less than 1 inch. Indexes, tables of contents, lists of figures/tables, and glossary of terms will not be counted toward the overall page count.

Graphic materials, standard commercial brochures or descriptions, or other standard product documentation that are attached in appendices or exhibits will not be counted against page limitations. However, evaluators cannot be expected to comprehend all material in exhibits whose content and relevance to the proposal description are not clearly integrated into the proposal.

Vendors are encouraged to print on both sides of the paper.

5.2 State of Colorado Request for Proposal Signature Page

The State of Colorado Request for Proposal Cover Page must be signed in ink by an Officer of the Vendor who is legally authorized to bind the Vendor to the proposal and comply with any other requirements identified in Section 2.8 above.

5.3 Transmittal Letter

All Vendors shall submit a Transmittal Letter positively stating their willingness and ability to comply with all work requirements, general contract requirements, and other terms and conditions specified in this RFP. If this is not the case, any exceptions or proposed deviations from requirements listed in this RFP must be described and explained. The CDOS reserves the right to reject any proposal indicating such exceptions or deviations. Additional requirements for the Transmittal Letter are that it:

- Must be on official business letterhead of the Vendor
- Should identify all material and enclosures comprising your proposal
- Must be signed by an individual authorized to commit the Vendor to the work proposed
- Must disclose intended use of any subcontracts
- Must acknowledge receipt of all amendments and addenda to this RFP
- Must disclose at least 2 electronic filing and/or electronic publication software implementations, serving as the prime contractor.

No reference is to be made to any pricing information or elements of cost. If any element of cost is referred to in the Transmittal Letter, the Vendor may be disqualified.

Vendors who fail to submit a Transmittal Letter may not be considered for award.

5.4 Other Solicitations / Potential Conflicts

Vendors are required to disclose all current or pending projects with the State of Colorado.

Vendor must include in the Transmittal Letter ALL potential and current conflicts related to this RFP and any other services related to this project.

5.5 Business Proposal

The Business Proposal should present a full and complete description of the qualifications and approach of the Vendor to carry out the requirements set forth in Section 4, Statement of Work. It is important that the proposal outline described below be followed since any deviation from this may disqualify a proposal. **(Also, cost information must not be disclosed in the Business Proposal**). The Business Proposal will include the following sections:

5.5.1 Executive Summary

The Executive Summary should provide the CDOS with an overall understanding of the proposal. Include a brief review of the proposal. The review shall be prepared in such a

manner as to make it understandable to individuals not familiar with the terminology peculiar to a project of this type.

Page Limit: 5 pages

5.5.2 Company Overview

Provide information about your company, its capabilities, and why it should be selected for this project. The overview should describe the kinds of projects your firm typically performs. Describe evidence of company stability and ability to perform required work for this project. Include items such as number of years in business, number of employees, employees with electronic filing and/or electronic publication software experience, and company location(s) (including any offices in Colorado). Vendor may provide any additional information that demonstrates the strengths they can bring to this project.

The Vendor shall indicate their form of organization (i.e., partnership, non-profit corporation, Colorado corporation, non-Colorado corporation, or some other structure). Non-Colorado corporations must register as a foreign corporation to conduct business in Colorado and appoint a resident agent to receive process. The Vendor further certifies that, it currently has a Certificate of Good Standing or Certificate of Existence to do business in Colorado. Proof of such certification shall be provided upon request by the CDOS.

This section should also include the following:

- Include a brief statement of compliance with the terms and conditions as set forth in Section 2: Administrative Information.
- Include a statement of compliance with the business requirements. It is important that the Vendor understand the size and scope of this application.
- Include any additional information you wish to add pertinent to your company doing business with the State of Colorado.

Page Limit: 5 pages

5.5.3 Relevant Business Experience

Vendors must provide adequate detail (including references) of at least 2 electronic pollbook software implementations, serving as the prime contractor. These implementations must have been completed during the past three years.

Vendors will provide written permission, with their proposals, for Vendor's references to release information to the State. Each reference must include both a primary and secondary client contact person, with current telephone, facsimile numbers and email addresses for each. For each referenced project describe if the project was completed on time and within the original bid amount. If not, identify time and overage. Additionally, disclose any litigation you have been involved with over contract performance. The CDOS reserves the right to contact and verify, with any and all firms with whom the Vendor has been known to have conducted business, the quality, and

degree of satisfaction for such performance. Vendors are responsible for providing references that have expressly agreed to be contacted by the CDOS.

Reference information should include:

- Number of internal users of the application system.
- Number of external users of the application system.
- Number of transactions processed (average daily; average annual).
- Number of change requests (including descriptions, resolutions and costs).
- Description of the architecture proposed and implemented including reason for difference.
- Information regarding the development tools, databases, operating system.
- References from each project.

Preference will be given to Vendors who demonstrate their experience with electronic pollbook software systems. Referenced projects should also demonstrate a proven capability in the following areas:

- Requirements gathering and definition
- System design
- System development
- Security
- Testing, and
- Project Management.

Page Limit: 20 pages

5.5.4 Prior Proposals

Vendor shall disclose any electronic pollbook software projects in which the vendor has submitted bids or proposals (as prime or sub) for consideration by a State/Territory. At a minimum, this information shall include:

- State/Territory
- contact name
- address
- date of response
- indicate result of bid
- Brief description

Page Limit: 10 pages

5.5.5 Project Approach

Provide a detail plan on the following aspects of the project.

Architecture

Utilizing the information provided in this RFP, provide a detailed plan regarding how you plan to implement the architectural portion of this project. Be specific regarding the recommendations regarding platform and architecture.

Utilizing the information provided in this RFP, provide the following:

1) Descriptions, supported by diagrams, showing the total overall system architecture (hardware and software) proposed.
2) Detailed description of the role of each component (or set of related components) in the total system architecture and how it, if applicable, contributes to:
    a) Capacity
    b) Scalability
    c) Expandability
    d) Availability
    e) Reliability
    f) Recoverability
    g) Administration
    h) Security
    i) Functional environment support
3) Description and requirements definition of any supportive components required to successfully execute any particular function, e.g. remote management, remote problem notification, etc.
4) A draft test/assurance plan to demonstrate all capabilities identified in 2) above. This test/assurance plan may be executed as necessary and after on-site installation. It must be executed as a part of the final implementation.

Software

Utilizing the information provided in this RFP, provide a detailed description of the software proposed for this system. Include a description of the customization efforts that may be needed.

Database

Provide information regarding the database recommended for this application. Please provide a detailed explanation for your recommendation.

Utilizing the information provided in this RFP, provide the following:

1. Database system recommended and any supporting capabilities (utilities, any special backup considerations, etc.).
2. Identify reasons for the recommendations.
3. If you feel that there are special considerations in the database arena, in order to have a successful implementation of the requirements, please describe in detail.

The CDOS will be the sole owner of the data that resides in the system. Provide an affirmation to include a statement of clear recognition that the CDOS:

1. Is the sole owner and custodian of all data in the system provided by the Vendor, and;
2. Shall have the unrestricted right to access and use all data in the system without interference by or assistance from the Vendor.

Application Development Tools

Provide information regarding the application development tools that the Vendor recommends for this application. In addition, provide notice of any upgrades or platform changes planned within the next 5 years.

If the proposed application development software is not the manufacturer's "state of the art", indicate why that choice was not made. Indicate your understanding of its "position" relative to expected offerings from the software manufacturer over the next two years and recommendations for possible transition of the application software to utilize advances of the new application development offering.

List and describe the function of all items proposed for the development tools.

Describe any specific hardware requirements needed to support functions and/or productivity of personnel regarding the development tools.

Proposed Test Strategy

The Vendor shall provide a description of their proposed test standards and methods for both their COTS product and custom development activities. The description must address test plan creation, test case/script generation, test phases, the execution of the test plan, and proposed participation by state staff.

The description of test plan execution should include the topics of results recording, defect handling, and regression testing. Any testing tools to be used by the Vendor should be mentioned.

Training

Describe the types of training, and the staff that should receive this training to maintain and operate the proposed system. Include types of skills and materials that would be needed/supplied.

In particular, describe how this would be executed in reference to Section 4.20 Training. The goal is to have confident staff and users, fully competent to support and operate the system.

Help Desk

Describe the process of the help desk in managing questions and issues from, CDOS, and operations. Describe the automation tools you will utilize to track help desk metrics. Include a discussion on expected response time replies to caller. Describe your methodology for sizing of the help desk. Describe the help desk implementation in your other state implementations.

Warranty

Describe what is included, excluded and the duration of the proposed warranty.

Annual maintenance

Describe what is included and excluded in the proposed annual maintenance agreement, if applicable.

Page Limit: 30 pages.

5.5.6 System Requirements

Information provided in this section will be used by the evaluation committee to determine how well the proposal meets the requirements of Colorado.

Statewide Electronic Pollbook System Requirements

The RFP Team has drafted a list of requirements that addresses the needs of CDOS. These requirements are listed in the "Statewide Electronic Pollbook System Requirements" document.

Utilizing the information provided in the requirements document, complete the table by following the instructions listed at the beginning of the document.

Page Limit: none (return completed table as directed in instructions)

5.5.7 Sample Project Materials

Vendors shall provide sample project reports, such as, design documents, functional descriptions of software, user manuals, training materials, test planning and execution materials, data conversion assessments and other communications from a electronic pollbook software project in which the vendor has participated which the vendor considers to be representative of their work, the quality of their work, and the level of communication and detail that the vendor provides. These **materials will be treated as confidential** and may be used to assess the format and detail that the vendor may provide if selected in Colorado. Respondents are encouraged to organize, label, title and/or describe these materials to indicate their content and purpose if such is not clearly apparent in the materials.

Page Limit: 30 pages

5.5.8 General Questions

The following is a list of questions regarding various aspects of the project. Please provide detailed answers to these questions.

1) The project may have another contractor whose function is to perform an Independent Verification & Validation (IV&V) of the project at various points. As part of that contract the IV&V agents will be making requests for information specific to the Colorado implementation and that address your company's general policies and procedure. Please provide an explanation on how you will handle requests for information regarding your "core" COTS product and the customized portion of the system. Specific examples of how this has worked on your current or past implementations would be beneficial.

2) Describe the documentation that you typically deliver to your client on a system application of this type, including documentation format (hardcopy, online, etc.), documentation type (technical, user, etc.) and frequency of update.
3) List and describe the risks identified on your previous electronic pollbook and/or voter registration software projects. Assign a risk value using a 1 for the lowest risk and a 10 for the highest risk. Explain what steps you took to mitigate each risk.
4) Describe the standard Quality Assurance/Quality Control (QA/QC) process that your organization used in the referenced projects. Describe how you would follow or tailor that process on this project.
5) Describe how your system complies with the final accessibility standards for electronic and information technology covered by section 508 of the Rehabilitation Act Amendments of 1998.

Page Limit: 30 pages

5.5.9 Project Organization and Preliminary Project Plan

CDOS anticipates that the vendor selected to fulfill this RFP will begin the effort no later than 21 calendar days after the award has been announced. CDOS expects the entire System to be implemented prior to April 30, 2014.

The Vendor shall deliver its proposed Project Organization and a Preliminary Project Plan.

Provide the required elements of the project plan as described in Section 4.10 - Proposed Project plan.

This section must provide a project organization chart listing by name, proposed personnel. It must also describe relationships between the Vendor and any subcontractors.

The Preliminary Project Plan should provide a roadmap of tasks, resources, and timing necessary to complete the work. The Preliminary Project Plan shall include but not be limited to the following:

- Tasks with scheduled start and completion dates
- Milestones
- Personnel assignments and estimated duration for each task. Time shall be listed for:
- Vendor personnel
- Required CDOS personnel (Vendor to define needed skill types or business area)
- Required technical personnel.

Page Limit: 10 pages

5.5.10 Proposed Staffing

The Vendor selected in response to this RFP must provide experienced, qualified professionals to insure the success of the project. Vendors must provide resumes and references for the personnel in their proposals who will bring expertise to this project.

Vendors should provide adequate documentation, references, and certifications to substantiate the expertise of those personnel, and state explicitly the amount of time such experts will work on this project in its various tasks.

The Vendor should list each individual proposed to serve the CDOS on this assignment, with a complete description of his or her role, responsibilities, and planned availability. Resumes must describe each individual's educational background, experience, other pertinent professional data, and should be sufficiently detailed to demonstrate an individual's qualifications and experience.

The Vendor must commit those personnel who are bid in the proposal will be assigned to the project, and will not be bid for other projects without the explicit written approval of CDOS. All "key personnel" identified on the project, must have a backup specified and available within a two week period.

The CDOS retains the right of approval over all proposed personnel, including potential substitutions to those proposed in response to this RFP. The Vendor commits to replace project personnel whose performance is unsatisfactory to the CDOS, with other personnel whose experience and skills are acceptable to the CDOS.

Should specific personnel proposed by the Vendor not be available for the project, the CDOS reserves the right to cancel any and all agreements with the Vendor.

The terms of this section shall apply to any and all vendors, including subcontractors, assignees, and successors involved in this project.

Page Limit: none

5.5.11 Financial Status

Vendors must provide company financial information. This information must include, at minimum, how long the company has been in business and whether or not it is a wholly owned subsidiary of another company. If the company is publicly traded, include a financial statement for the last two (2) years, which includes, at minimum, a profit and loss statement and a balance sheet. If the company is not publicly held, submit a copy of the company’s most recently audited financial statement and organization/financial structure of the company. Unaudited financial statements or Dun and Bradstreet reports alone are unacceptable, and if submitted without additional support documentation, may be grounds to eliminate the company from consideration. All financial information (except public information for a publicly held company) will be treated as confidential and shall be used for this proposal only.

The Vendor shall also include a statement of the Vendor's other contractual obligations that might have an influence on the capabilities of the Vendor to perform the conditions of the contract (i.e., shared personnel) or, whose financial condition is deemed to be a risk to the CDOS for successful performance of the contract.

The CDOS may disqualify from consideration any Vendor who is involved in bankruptcy proceedings.

Page Limit: none

5.6 Cost Proposal

The quoted price must include a proposed contract maximum amount to be billed. It is highly encouraged that the vendors provide as much line item detail as possible in the costs tables.

Vendors must submit cost proposals in the format identified in the Cost Tables spreadsheet. Please note that the Cost Proposal must be:

a) submitted separately from the business proposal in a manner described in Section 5; and

b) submitted in the pre-formatted Microsoft Excel spreadsheet file provided.

Software Cost Table

This table is designed to identify all the software costs associated with the proposed system. Enter the proposed software components on each line with the applicable information. Vendor may add more rows if needed.

Project Labor Cost Table

This table is designed to identify all the project labor costs associated with the implementation of the proposed system. Enter the proposed labor activities on each line with the applicable information. Vendor may add more rows if needed.

Operational Labor Cost Table

This table is designed to identify all the operational labor costs associated with operating and maintaining the proposed system. This cost information must be provided regardless if the vendor is proposing an optional hosting solution. Enter the proposed labor activities on each line with the applicable information. Vendor may add more rows if needed.

Hourly Rate Table

This table is designed to identify the rates that the Vendor will charge for any work identified and approved beyond the scope of this RFP. Enter the proposed labor description on each line with the applicable information. Vendor may add more rows if needed.

Miscellaneous Cost Table

This table is designed to identify all the miscellaneous costs associated with the proposed system. Enter the various components on each line with the applicable information. Vendor may add more rows if needed.

Total Cost Table

This table accumulates all the cost from the previously listed tables, excluding the Hourly Rate Table. This table is formula driven, thus, **the Vendor should not modify this table**.

Page Limit: none

Vendors must submit cost proposals in the format identified in the Cost Tables. The quoted price must include a proposed contract maximum amount to be billed. It is highly encouraged that the vendors provide as much line item detail as possible in the costs tables.

5.7 Design, Performance and Testing Materials

Materials submitted in response to the following questions must be separate from other portions of your response as stated in the Section 5 overview.

5.7.1 System Architecture

Please provide detailed schematics and narrative descriptions of your system architecture.

Page Limit: none

5.7.2 Application Architecture

Please provide schematics and narrative descriptions of your application architecture.

Page Limit: none

5.7.3 Platform Architecture

Please provide descriptions of your system platform. If your solution has both centralized and remote components (such as tablet-based clients connecting to a centralized infrastructure), please describe both.

Page Limit: none

5.7.4 Static Code Analysis

Have you performed static code analysis on your electronic pollbook solution? If “yes” please provide results from this assessment.

Page Limit: none

5.7.5 Vulnerability Assessments

Have you performed vulnerability assessments of your electronic pollbook solution and accompanying technologies? If “yes”, please provide information on these assessments.

Page Limit: none

5.7.6 Load or Stress Testing Assessments

Have you performed load or stress testing on your electronic pollbook solution and accompanying technologies (e.g., peak load, simultaneous user requests, simultaneous database connections, memory leaks)? If "yes", please provide information on these assessments.

Page Limit: none

5.7.7 Performance Testing Assessments

Have you done performance testing on your electronic pollbook solution and accompanying technologies (e.g., capacity, scalability, latency at various load levels)? If "yes":

5.7.7.1 Please provide information on these assessments.

5.7.7.2 Please provide information on your performance testing acceptance criteria, such as:

5.7.7.2.1 Response time (e.g., less than 3 seconds to display).

5.7.7.2.2 Throughput (e.g., must support 100 transactions per second).

5.7.7.2.3 Resource utilization. (e.g., the amount of resources your application is consuming, in terms of processor, memory, disk input output (I/O), and network I/O).

5.7.7.2.4 Maximum user load (i.e., how many users can run on a specific hardware configuration).

5.7.7.2.5 Business related metrics (e.g., volume at normal and peak values).

5.7.7.3 Please provide information on your performance test scenarios (e.g., transaction scenarios, workload level).

5.7.7.4 Please provide information on your performance test results.

Page Limit: none

5.7.8 Penetration Testing Assessments

Have you performed penetration tests of your electronic pollbook solution and accompanying technologies? If "yes", please provide information on these pen tests.

Page Limit: none

SECTION 6: PROPOSAL EVALUATION

6.1 Introduction

The CDOS will conduct a comprehensive, fair and impartial evaluation of proposals received in response to this Request for Proposal. The objective of the final evaluation is to determine the proposal that most effectively meets the CDOS goals and requirements. The contract for this project will be awarded to the Vendor whose proposal, conforming to the RFP, will be most advantageous to the CDOS and the State of Colorado, price and other factors considered.

A RFP Evaluation Committee will review and score submitted proposals to determine which (not limited to):

- demonstrates experience
- best meets RFP requirements
- has reasonable costs
- minimizes risk of failure to the CDOS
- has adequate finances and resources to successfully complete the project
- demonstrates a sound approach
- has adequate, qualified personnel
- shows good understanding of the requirements
- requires only limited clarification

6.2 Evaluation Process

The CDOS reserves the right to award on receipt of initial proposals. If award is not made upon receipt of initial proposals, the CDOS will provide Vendors remaining in the competitive range with written requests for clarifications/notice of deficiencies in their proposals. Vendors will be provided a date at which oral presentations and demonstrations will be heard. Each oral presentation and demonstration is planned to be eight (8) hours in duration. The presentation shall consist of a vendor briefing concerning its technical approach and must also address clarifications and deficiency items identified by the CDOS that may lead to discussions. Guidelines regarding the oral presentations will be distributed to those Vendors remaining in the competitive range.

Vendors may be given an opportunity, after the conclusion of the oral presentations, to submit a best and final offer (BAFO). Vendors will be informed in writing of the date by which best and final offers are due. Vendors shall make any revisions the CDOS deems necessary to clarify or correct weaknesses in their proposal. Revisions shall be made by “change page” to proposals, including pricing. The CDOS does not require complete, substantial proposal rewrites. Vendors are cautioned not to make changes in the technical approach or make price/cost revisions that are not clearly explained and/or justified in any proposal revision. Vendors assume the risk that proposed revisions be adequately explained so the CDOS understands the nature of the revisions and the risk to the CDOS from unreasonable forecasts of contractor costs.

An Evaluation Committee will be assembled that consists of cross-disciplinary representatives from within CDOS and possibly outside stakeholders, including program personnel and information technology professionals. Evaluators will have an opportunity to revise their scores and comments based on deliberative discussions.

The relevance and comprehensiveness of past experience and qualifications will similarly be evaluated to assess the risk of either unacceptable or late performance.

While a numerical rating system will be used to assist the evaluation committee in selecting the competitive range (if necessary) and making the award decision, the award decision ultimately is a business judgment that will reflect an integrated assessment of the relative merits of the proposals using the factors and their relative weights.

Vendors should not assume that they will have an opportunity for oral presentations or revisions of proposals, so they should submit their most favorable proposals as their initial proposal. If award is not made on receipt of initial proposals, Vendors in the competitive range (those most responsive to the requirements) will be provided an opportunity to make an oral presentation as part of the discussions. The competitive range determination will be based on the written proposals, so Vendors are cautioned to insure that their proposals adequately convey the soundness of their approach and understanding of the requirements.

6.3 Evaluation Procedure

Evaluation Phase 1- Administrative (Pass/Fail)

Proposals will be evaluated to determine if the administrative requirements have been met. These requirements include:

1. Proposals have complied with the bid due date and time
2. The requested format and number of copies are adhered to
3. Page limits and font size meet requirements
4. The Request for Proposal Cover Page meets the content and other requirements
5. The Transmittal Letter is enclosed and meets the content and other requirements
6. Separate packaging rules are followed

Vendor shall be considered noncompliant and may be eliminated from further evaluation if information is incomplete.

Evaluation Phase 2 – Technical and Business (75% weight factor)

Only those vendors who pass Evaluation Phase 1 will enter Evaluation Phase 2. Phase 2 will result in a numerical score based upon the information provided in the Business Proposal, the “Statewide Electronic Pollbook System Requirements” document, and the information submitted in response to Section 5.7; the information is clear and concise; and how well it meets the requirements as defined in the sections.

All information requested must be provided.

Evaluation Phase 3 – Cost Evaluation (25% weight factor)

Each proposal will be assigned points based on Cost Proposal. CDOS will use annualized on-going costs in the cost evaluation of the proposal.

Evaluation Phase 4 – Initial Points Calculation

The points assigned in Phases 2 and 3 will be added together to produce an initial point score for each proposal. A determination will be made to which vendors, offering the most advantageous proposal, remain in the competitive range.

Evaluation Phase 5 – Oral Presentations and Demonstrations

At the sole option of the CDOS, as few as two (2) vendors or as many as six (6) vendors (selected in rank order) will be eligible for further evaluation in this phase. If requested by the CDOS, vendors shall provide an oral presentation concerning the overall proposal. Selected vendors must be prepared to provide a presentation at a Denver metro location, during the timeframe listed in the Schedule of Activities for this RFP. Vendors will be notified to prepare the oral presentation to present within the timeframe as described in the table in Section 2.5.

These presentations will provide vendors with an opportunity to present information to the Evaluation Committee that the committee will use to award points to the proposal based on the following:

- The Vendor's grasp and understanding of the project as a whole.
- The Vendor's overall approach to project execution and management.

The State will be conducting an Architecture Assessment Validation (AAV) on the vendor's proposed architecture during the Oral preparation period. The State expects complete cooperation with the AAV vendor during that period. The vendor will need to make available, to the AAV vendor, both the technical and project management resources proposed. The vendor should expect both questions and follow-up interviews during the period.

The Vendor's complete solution shall be made available to the evaluation team for a period of five (5) business days, independent of Vendor or Representative being present. The Vendor shall provide two (2) workstations and a server (if applicable) for this demonstration period. These workstations will reside in a secure room at the CDOS offices. CDOS will also consider other similar options for the full demonstrations. The solution is not expected to address ALL requirements in this RFP, but only those requirements the Vendor has deemed as "satisfied" in their response. The purpose of this activity is to allow the evaluation team to "test drive" the solution to gain a better understanding of the application.

If a Vendor is unable or unwilling to provide this demonstration, they must provide an explanation in their proposal.

Evaluation Phase 6 – Final Points Calculation

The initial points assigned in Phases 2 and 3 will be re-evaluated and subject to adjustments based on Phase 5 activities. The adjusted points will be added together to produce a final point score for each proposal.

6.4 Notice of Intent to Award

Award shall be made to the Vendor offering the most advantageous proposal, price and other factors considered.

The CDOS anticipates making a proposal selection within 20 days after closing date for receipt of proposals. Upon selection, and after required approvals, the CDOS will post a Notice of Intent to Award on the CDOS Web site.

SECTION 7: APPENDICES

7.1 APPENDIX A: Colorado Department of State Acceptable Use Computing Policy

ACCEPTABLE USE COMPUTING POLICY

Colorado Department of State (Secretary of State's Office)

I. Introduction
   a. Information's confidentiality, integrity, and availability are critical to the Colorado Department of State's (CDOS) operation and purpose. With the daily increase of society's use of and dependence on Information Technology, it is imperative that employees, contractors, and others ("users") use the computer systems responsibly. Even inadvertent misuse of CDOS computer systems can cause enormous operational, legal, and monetary problems for the Department.

II. Purpose
   a. The purpose of this Policy is to set forth a clear and concise standard to assist users in the use of their computers, terminals, and other computing devices on the CDOS network or containing CDOS information. Also set forth in this Policy are standards for new equipment requests, new software requests, licensing standards, help desk support information, and other information to make the computing experience the best possible.

III. Policy
   a. Scope
      i. This Policy is intended to meet the State of Colorado's Cyber Security Policies as required by the State. The State's Cyber Security Policies can be found on the State of Colorado's web site at www.colorado.gov.
   b. User Responsibilities
      i. General
         1. Computer resources and data are to be used for departmental business only. Limited personal use is permitted as outlined in the Employee Handbook. These resources are vital to the function and continuance of the organization. Access to these resources is granted to employees and their designated contractors on a need-to-know basis as required to perform their job functions or contractual obligations. Unauthorized attempts to use these resources will be grounds for disciplinary action, to include but not limited to suspension, termination, and legal action.
         2. CDOS users are required to adhere to Federal, State, and local laws. Users are required to adhere to the State of Colorado's

Cyber Security Policies as well as the Department's Employee Handbook, Cyber Security Policies and Acceptable Use Policy.

ii. Data Ownership
    1. Ownership of data will reside with the Department or Division Director responsible for the data. Access permissions must be granted by the data owner before a user may attempt access.

iii. User ID and Password
    1. Each user will be given a unique user ID for access to the network and other resources.
        a. Each Logon-id will have a password that is set by the user upon initial logon. Passwords should be chosen carefully and kept private so that the logon-id will not be compromised. Any suspected compromise should be immediately reported to a user's supervisor who in turn will report the incident to the Department's Information Security Officer (ISO). The password is required to be 8 characters long at a minimum and must consist of a combination of at least three out of four of the following: uppercase letters, lower case letters, numbers, and symbols. After a user or other individual attempts to log on to an account more than 5 times with the incorrect password the account will be locked out. To reactivate the account the user will need to contact the Help Desk at 303.894.2200, extension 6680.
        b. User passwords are to be kept strictly confidential. Users may not give their password to anyone, including supervisors or Information Systems personnel. Users may not write down their ID and/or password since another person may find it and use it inappropriately. Each user is responsible for all actions associated with this Logon ID and password and will be held accountable for any improprieties regarding its use. Penalties for sharing passwords can be severe and could include disciplinary action up to and including termination.
        c. To reduce the possibility of a system being compromised, or a user obtaining a password they are not permitted to use, user account passwords will expire every 90 days. When the password expires the user will be prompted to provide a new password; the new password must be entered twice for confirmation.
        d. To ensure additional security, users should
            i. Log off of the computer system or lock the screen on their computer if they are going to be out of sight of their computer.
            ii. Protect their password from disclosure to others.

iii. Choose passwords that are not obvious. A good password includes a combination of upper case letters, lower case letters, numbers, and symbols. Passwords should never consist solely of dictionary words, even from foreign language dictionaries. Dictionary words, even with symbol substituted characters, repeated words, or numbers on the end, can often be easily compromised with a simple password guessing program.
iv. Not write their passwords down or leave the password in a written format in their work area.

e. Users are allowed to change the password on their account one day after the initial password change. If a user forgets his or her password, contact the Help Desk at 303.894.2200, extension 6680. A randomly generated password will then be assigned which the user is required to change immediately.
f. Users may not try in any way to obtain a password for another user's account.
g. Administrators will create Logon-id's with access privileges as defined by the data owners. All new user accounts must be assigned a randomly generated password meeting the password policy requirements and the system must or administrator must assure the password is change by the user the first time they login to the system. The administrator is responsible for security implementation and will ensure the necessary resources for maximum system availability. Reasonable controls such as audit trails and separation of function will be employed wherever possible. Experienced security auditors will periodically verify the accuracy and control of the security system.
h. Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.
i. Users must not use the network resources to gain or attempt to gain unauthorized access to remote computers.

iv. System File Shares/Drives

1. Each Division will have a shared information drive. The Secretary of State and the Division's Director will set security policies for access to Division's shared drives. Currently, users have access to the Division's shared drive, but may have restrictions set to "Read Only" rather than "Read, Write" permissions. Only users given permission to view directories within the drive, the IS

Administrators responsible for maintaining the server, and any other party within the state system with the legal authority to view the information will have permission to access the files. Under no circumstance will Systems Administrators view the contents of the files, beyond what is necessary to perform their assigned job function, secure the files and ensure data back-up, without the permission of the department head, data owner or appropriate supervising authority.

2. Home Directories
    a. Each user will be assigned a Home Directory which will only be accessible to that user, the IS administrator responsible for maintaining the server, and any other party within the state system with the legal authority to view the information.
    b. Under no circumstance will Systems Administrators view the contents of the files, beyond what is necessary to perform their assigned job function, secure the files and ensure data back-up, without the permission of the department head, data owner or appropriate supervising authority.
3. File Safety
    a. In order to ensure file safety, users should store mission critical data on their assigned network drives; routine backups are performed on network drives and it provides the surest method of protecting files. Storing of data to floppy disks, flash drives or the local hard drives is susceptible to loss of critical files with little or no chance of recovery from hardware failures or loss of disk resources.
    b. Storage of data to local drives and media is not backed-up and will not be recoverable if lost or damaged.
    c. In the event that a computer is having any technical difficulties (i.e., hardware failure, basic software glitches, poor performance) or needs an update, the Information Systems Division reserves the right to reinstall software and/or the operating system which ultimately could result in the loss of data stored on any local drives.
    d. Any information containing credit card numbers, confidential information or personally identifiable information (PII) should not be e-mailed, transmitted or stored on removable media without proper encryption as required by State of Colorado policies and the Department of State's Information Systems Division.

v. Internet and Systems Use
    1. The Internet will be used to conduct Department business. Limited or occasional personal use of the Internet is permitted as outlined in the Employee Handbook. Individual job functions will

determine the Internet services approved for an individual. The rule of "least privilege" (only necessary Internet services will be granted to perform a particular job function) will be used in granting access to Internet services. Further, Internet addresses of sites which contain racial, sexual, obscene, harassing, criminal, subversive or other information which violate local, State, Federal laws or regulations, or CDOS policies and procedures may be blocked.

2. Individuals who have Internet access will only use the IS Department-configured Internet Gateway and the State Of Colorado's Internet Service Provider. The only exceptions to this Policy are those cases where connectivity to a customer requires access to a specific Internet Service Provider (e.g. CompuServe, America Online, etc.). Alternate Internet access will not be approved if the necessary services can be provided through the currently configured Internet Gateway.
3. Malware (Virus, Trojans, Worms and other Malicious Software)
    a. The threat of a malware infection can arise from downloading files from the Internet, loading data into your computer from a diskette/flash drive, visiting a malicious Internet site, bypassing a system's security controls, or executing an e-mail attachment. All personal computer systems are loaded with antivirus and firewall software. Users may not disable the firewall or anti-virus software on the systems provided for their use. Intentionally or willfully violating these security controls without proper approval may result in disciplinary action.
4. CDOS Systems and Internet access may not be used to:
    a. Communicate unethical, racial, sexual, obscene, harassing, or improper material.
    b. Send or willfully receive any unethical, racial, harassing, obscene, or sexual software, data documents, pictures or videos.
    c. Send outside the Department any sensitive, proprietary, confidential, or Personally Identifiable Information without a Director's or her/his designee's authorization.
    d. Send or download any software, including but not limited to shareware, freeware, or browser controls without proper Information Systems approval.
    e. Send or download copyrighted material unless authorized by the copyright holder.
    f. Create false or misleading information (either individually or by masquerading).
    g. Violate Federal, State, or local laws or regulations.
    h. Violate Department policies or procedures.
    i. Disrupt Department or other site's operations.

j. Abuse the rights of others.
k. Engage in activities in support of/or opposition to candidates or campaign issues.
l. Play Internet Games
m. Use chargeable Internet Service Provider(s) services or fee for services or downloads from other sites for personal use.
n. Access proxies or other services in order to bypass the Department's security controls.

5. Restricted Internet Facilities
    a. Because of the risk to data confidentiality, integrity and accessibility, the following Internet Facilities will be, at a minimum, restricted: Rlogon (Remote Log on), FTP (File Transfer Protocol), Telnet, NFS (Network File Service), and RFS (Remote File Service).
6. Revoking of Use
    a. The Department reserves the right to revoke at any time the use of the Internet and/or Remote Access.
7. Office Representation on the Internet
    a. Office communications through the use of social networking sites
        i. All communications made through social networking sites on behalf of or concerning the Secretary of State, the Department of State or any division within the Department shall be made through or with the permission of the Public Information Officer. This includes communications through "blogs", Twitter, Facebook and any other similar social networking site. However, this does not include the use of collaborative online tools like Google Groups or ListServ, whose use must be approved via a Standard Information Systems Request and must abide by State of Colorado policies regarding Personally Identifiable Information (PII) and Confidential information.
    b. Use of social networking sites during business hours
        i. The Department believes these sites can help to boost or maintain employee morale, as long as they are used appropriately. Personal social networking sites may be accessed during normal business hours as part of an employee's scheduled or authorized lunch or break times. In order to access these sites, employees shall abide by all office communications and Internet policies including "Office communications through the use of social networking sites," and be advised and current of all security threats related to these sites.

ii. Accessing these kinds of sites during business hours is a privilege, and abuse of these policies may result in blocked access, suspension, or even termination.

c. Personal use of social networking sites
   i. Whether communicating with someone over the phone or over the counter, each employee in the Department of State needs to remember that s/he is representing the Secretary of State. This representation can extend outside the office to personal appearances at meetings, conferences and seminars and on social networking sites. Employees need to exercise caution when posting language, videos, or pictures on any social networking sites that could reflect poorly on the Office or the Secretary of State. These sites include any blogs, Twitter, Facebook, or other similar social networking site.
   ii. The use of State e-mail addresses in non-business related forums such as newsgroup postings, discussion boards, or instant messaging is expressly prohibited.

vi. Department and Individual Liabilities

1. The Department may be financially liable for copyrighted or licensed material (documents, software, etc.) which are used by Department employee(s) without the permission of the copyright or license holder. If the Department becomes liable by an employee's use of copyrighted or licensed material without the permission of the copyright or license holder, the Department may initiate disciplinary action as well as seek restitution from the responsible party.

   Further, the Department may be financially liable for Internet services provided by an Internet Service Provider (ISP) or from any site on the Internet which charges a fee for service/download when an employee is accessing that site in the performance of their assigned duties. If use of an ISP or another site's service is of a personal nature, and the Department is charged, the individual using these services will be held financially liable. Individuals who download shareware or software without authorization, or circumvent proper virus checking using Internet or Remote Access which have an adverse affect upon confidentiality , data integrity , or availability of the Department's Information Systems (PC's, servers, network, etc.), may be subject to disciplinary action as well as be financially liable.

Licensed or copyrighted material (documents, data, or software) downloaded either through the Internet or by Remote Access which has not been approved is not permitted.

It should be noted that initially, shareware or other software may have no fee, but there may be hidden costs, such as future upgrades which may require fees, incompatibility with the standard desktop environment, and maintenance and supportability of the software. These factors will be considered when a Division requests approval for software downloads.

vii. Remote Access
    1. Due to the serious nature of a possible Internet security breach, Remote Access to any of the Information Technology systems is strictly determined by the Secretary of State and the IS Division Head.
    2. No personal use of the network is permitted via Remote Access.
    3. Users are responsible for their network use and should never relinquish control of their systems to non CDOS technical support, vendors, or other Internet users without proper supervision. Users shall not allow another individual to perform illegal activities, obtain confidential information, or compromise the system in any way via remote control or remote access software.
    4. Remote Access and Remote Control software is only permitted after approval from Information Systems.

viii. E-mail
    1. All e-mail sent to and from a departmental assigned e-mail account (user@sos.state.co.us) is property of the state. Caution should be used when receiving an e-mail with an attachment. All attachments will be scanned with virus scanning software prior to opening. Users should contact the help desk if there is any question as to the security of a document.
    2. The use of State e-mail addresses in non-business related forums such as newsgroup postings, discussion boards, or instant messaging is expressly prohibited.
    3. E-mail may not be used to:
        a. Communicate unethical, racial, sexual, obscene, harassing, or improper material.
        b. Send or willfully receive any unethical, racial, harassing, obscene, or sexual software, data, documents, pictures or videos.
        c. Conduct activities for personal profit or commercial purposes.
        d. Gossip or gamble.

a. Send or receive chain letters or emails.
b. Send outside the Department any proprietary or confidential information without a Director's or her/his designee's authorization.
c. Send or receive copyrighted material unless authorized by the copyright holder.
d. Create false or misleading information (either individually or by masquerading).
i. Violate Federal, State, or local laws or regulations.
j. Violate State Government or Department policies or procedures.
k. Disrupt the Department's or an external site's operations.
l. Abuse the rights of others.
m. Engage in activities in support of or opposition to candidates or campaign issues.
n. Send or receive any software (unless required by the position and prior approval is obtained from the IS Division).

ix. Privacy

1. When using unsecured systems such as the Internet or any telephony communication facility such as Remote Access, information should not be considered private. Further, all transmissions of information, data, and messages sent through the Internet or Remote Access Services are considered to be business records and are treated as such. All business records are subject to inspection, review, or disclosure without prior notice, or as required by law.
2. The Colorado Department of State reserves the right to access and disclose all information, data, and messages that are sent, received, or stored through its Internet Access and Remote Access Services.

x. Disciplinary Action

1. Improper use of the Internet or Remote Access can be used as grounds for corrective and/or disciplinary action to include revocation of access, financial liability, civil or criminal prosecution, and termination.

xi. Incident Response

1. If an event, such as a seemingly malicious pop-up, a virus warning, or other suspicious activity occurs users are required to report the incident to the Help Desk. The Help Desk will then report the incident to the Information Security group. Some examples of incidents include:
    a. Unusual pop-ups and/or virus warnings.
    b. Suspicious callers attempting to obtain un-authorized information such as a user's password or other personnel information.

c. Suspected attempts (either failed or successful) to gain unauthorized access to a system or its data by unauthorized parties.
d. Systems experiencing slow or abnormal behavior that appear to be under a denial of service attack.
e. The unauthorized use of a system for the processing or storage of data.

xii. Security Infractions and Monitoring
1. If for any reason a Supervisor, system administrator, or computer security personnel suspect that these policies are being compromised, a user's computing activities may be monitored without any notification to the user. This includes, but is not limited to, Internet access, file access, and e-mail activity.
2. In the event that a user is attempting to compromise security on a system, disciplinary action may be taken including revocation of access, financial liability, civil or criminal prosecution, and termination.
3. Security personnel and administrators will audit systems access, review system and application logs, search for security violations, monitor Internet traffic, perform systems penetration tests, and carry out other security related functions on all systems on a regular basis as permitted by the Chief Information Officer (CIO).

xiii. Hardware/Software Requests
1. No employee or contractor of the Department shall engage in any activity that violates Federal, State, or local laws with respect to intellectual property rights, terms of software license agreements, or other policies pertaining to computer software. All software and hardware installed on a device connected to the Department of State's network is required to have written approval from the Information Services division and will be entered into the Department's database for tracking. This is a critical step in order to have both effective desktop support and proper licensing. Any hardware and/or software which has been installed without the proper hardware/software request form and a state-owned commercial license will not be supported and is subject to immediate deletion and/or removal as well as possible disciplinary action
2. Removable media and hardware that is not issued by the Department with the proper security controls is not permitted to connect to the Department's computer systems. Some examples include personal USB drives, external storage devices, mobile phones, I-Pods, MP3 players, tablets, and any other device that can be used for portable storage. This requirement is in place to prevent loss of confidential information, possible malware infections, as well as allow for proper system support.

c. Employment Termination

i. Upon termination of employment for any reason, Information Systems must be notified by the supervisor or Division Directory immediately. The supervisor and/or Division Director should provide notice to Information Systems with specific dates and times for systems access removal including, but not limited to the following:
    1. Building and Department Door Card Access
    2. Remove Access
    3. Windows, UNIX, and other Network Systems access.

d. Information Systems Help Desk
    i. If you have questions concerning this Policy or other systems questions please contact the Help Desk via phone at extension 6680 or e-mail at ithelpdesk@sos.state.co.us.

As an employee, contractor or other user of the Colorado Secretary of State's computing facilities, I acknowledge that I have read and understand the Acceptable Use Computing Policies and Procedures.

I agree to strictly abide by these policies and procedures and acknowledge that when an instance of non-compliance is suspected or discovered, proper disciplinary action may be taken, up to and including termination in accordance with state regulations. Criminal or civil action may be initiated where appropriate.

Employee Name (printed)	Division (printed)
Employee Signature	Date
Human Resources Signature	Date

7.2 APPENDIX B: Colorado Department of State Privacy Agreement

Colorado Department of State

Policy Regarding Employees' Security and Privacy; Disclosure of Employees' Last Names

The Colorado Secretary of State places great importance on the security and privacy of each employee of the Department of State. Each employee has, to a lesser or greater degree, continual contact with the Department's customers and with the public at large. Therefore, the potential exists that the security and privacy of the employee might be compromised if the employee were required to disclose personal information about the employee, including the employee's full name, to customers or the public.

In order to further safeguard the employee's security and privacy, it is the policy of the Department of State that no employee shall be required to disclose more than the employee's first name when communicating with the Department's customers and with the public at large and, further, it shall be the option of the employee whether to disclose the employee's full name or other personal information.

Date

_____

Scott Gessler,

Colorado Secretary of State