Department of State

Request For Proposal
#CDOS-Elections-RFP-2018-001 Risk-limiting Audit software system

February 22, 2018

The Colorado Department of State (CDOS) is soliciting proposals to select a Contractor to develop enhancements to the web-based risk-limiting audit system for Colorado election officials to use in auditing primary, coordinated, and general elections.

(Exhibits attached as separate documents)

Section 1: Introduction

1.1 INQUIRIES: This Request for Proposal (RFP) is being conducted under the Elective Officer Exemption, section 24-2-102(4), C.R.S., and outside the State Procurement Code. Unless otherwise noted, prospective Contractors may make written or e-mail inquiries concerning this RFP to obtain clarification of requirements. Inquiries should be clearly identified in the subject line as relating to RFP: CDOS-Elections-RFP-2018-001. E-mail is the preferred method for vendors to submit inquiries. No inquiries will be accepted after the date and time indicated in the Schedule of Activities.

E-mail or mail all inquiries to: Brad.Lang@sos.state.co.us

Brad Lang
Controller & Budget Director
Colorado Department of State
1700 Broadway, Suite 200
Denver, CO 80290

Responses to all inquiries will be published in a timely manner on the Voting Systems page of the CDOS website at https://www.sos.state.co.us/pubs/elections/VotingSystems/VSHomePage1.html.

1.2 MODIFICATION OR WITHDRAWAL OF PROPOSALS: Proposals may be modified or withdrawn by Contractors prior to the established due date and time.

1.3 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 Contractor to ensure that the proposal is received by the CDOS on or before the proposal due date and time. Contractors mailing their proposals shall allow sufficient mail delivery time to ensure receipt of their proposals by the time specified. The proposal package shall be delivered or sent by mail to:

Attn: Brad Lang
Controller & Budget Director
Colorado Department of State
1700 Broadway, Suite 200
Denver, CO 80290

The State of Colorado Request for Proposal Cover/Signature Page MUST be signed in ink by the Contractor or an officer of the Contractor legally authorized to bind the Contractor to the proposal. The Cover/Signature Page is attached as Appendix A.

Proposals which are determined to be at a variance with this requirement may not be accepted. Proposals must be submitted and sealed in a package showing the following information.

CONTRACTOR COMPANY NAME
RFP: CDOS-Elections-RFP-2018-001 Risk-limiting audit software system

The Colorado Department of State desires and encourages that proposals be submitted on recycled paper, printed on both sides.

1.4 ADDENDUM OR SUPPLEMENT TO REQUEST FOR PROPOSAL: In the event that it becomes necessary to revise any part of this RFP, an addendum/amendment will be published on the Voting Systems page of CDOS's website

athttps://www.sos.state.co.us/pubs/elections/VotingSystems/VSHomePage1.html. It is incumbent upon Contractors to carefully and regularly monitor this site for any such postings.

1.5 ORAL PRESENTATIONS/SITE VISITS: Contractors may be asked to make oral presentations or to make their facilities available for a site inspection by the evaluation committee. Oral presentations will be at the expense of the Contractor; if site visits are required, Contractors will be responsible for coordinating such visits.

1.6 ACCEPTANCE OF RFP TERMS: A proposal submitted in response to this RFP shall constitute a binding offer, and the proposal submitted by the Contractor who is awarded this project shall be the basis for the subsequent contract with said Contractor. Acknowledgment of this condition shall be indicated by the autographic signature of the Contractor or an officer of the Contractor legally authorized to execute contractual obligations.

1.7 RESERVED

1.8 CONFIDENTIAL/PROPRIETARY INFORMATION: Any restrictions of the use or inspection of material contained within the proposal shall be requested prior to the submission of the proposal itself. Written requests for confidentiality shall be submitted by the Contractor prior to the proposal submission date. The Contractor must specifically state the elements of the proposal that are considered confidential or proprietary. CDOS will make a written determination as to the apparent validity of any written request for confidentiality, and the written determination will be sent to the Contractor.

Requests that are granted shall use the following format:

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

After award, the offers shall be open to public inspection subject to any continued prohibition on the disclosure of confidential data, C.R.S. Title 24, Article 72, Part 2 as amended.

1.9 RFP RESPONSE MATERIAL OWNERSHIP: All material submitted regarding this RFP becomes the property of the State of Colorado. 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 C.R.S. Title 24, Article 72, Part 2 as amended.

1.10 PROPOSAL PRICES: Estimated proposal prices are not acceptable. Best and final offers may be considered in determining the apparent successful Contractor. The best and final offer will be used as the basis for the terms of the subsequent contract with the successful Contractor. Proposals shall be firm for a period of not less than 180 calendar days.

1.11 EVALUATION: The evaluation will identify the proposals that most effectively meet the requirements of this RFP. The work will be offered to the Contractor whose proposal conforms to the RFP and is most advantageous to the State of Colorado, when price and other factors are considered.

The State of Colorado will conduct a comprehensive, fair and impartial evaluation of each proposal received. CDOS will be responsible for ensuring that:

- The Contractor's proposal complied with the due date and time.
- The Contractor's “State of Colorado Request for Proposal Cover/Signature Page” meets content and other requirements.
- The Contractor included the appropriate number of proposal copies.

The Evaluation process is outlined in Section 5.0

1.12 PROPOSAL SELECTION: Upon review and approval of the evaluation committee's recommendation for award, the Colorado Department of State will issue a "Notice of Intent to Make an Award" and will notify all Contractors by email. A contract must be completed and signed by all parties concerned on or before the date indicated in the Schedule of Activities. If this date is not met, the State may elect at its sole discretion to cancel the "Notice of Intent to Make an Award" and make the award to the next most advantageous Contractor.

1.13 AWARD OF CONTRACT: The award will be made to the Contractor whose proposal conforms to the RFP and is considered the most advantageous to the State of Colorado, when price and other factors are considered.

1.14 PROPOSAL CONTENT ACCEPTANCE: The contents of the proposal (including persons specified to implement the project) of the successful Contractor will become contractual obligations if acquisition action ensues. Failure of the successful Contractor to accept these obligations in a contract may result in cancellation of the award and such Contractor may be removed from future solicitations.

1.15 STANDARD CONTRACT: CDOS incorporates standard State contract provisions (General and Special Provisions) into any contract resulting from this RFP. A model contract may be viewed at the Colorado State Controller's website at https://www.colorado.gov/pacific/osc/contractgrant-forms (Please refer to the model "Personal Services Contract".)

By submitting a RFP, the Offeror confirms its willingness to enter into a contracting document containing the terms and conditions of the Standard Personal Services Contract and the requirements of this solicitation without exception, deletion, qualification, or contingency. CDOS will not consider any changes, additions, or exceptions to the standard terms and conditions.

Should the contract not be completed and agreed to by both parties within 30 calendar days following the issuance of a draft contract to the successful Offeror for review, through no fault of the Department's, the Department, at its sole discretion, may elect to cancel the existing award announcement and make an award to the next most advantageous Offeror.

The Department will not accept any RFPs that are conditional on acceptance of modified state terms and conditions.

1.16 RFP CANCELLATION: The State reserves the right to cancel this Request for Proposal at any time, without penalty.

1.17 STATE OWNERSHIP OF CONTRACT PRODUCTS/SERVICES:

1. Proposals submitted become the property of the State of Colorado upon the deadline for submission. All products/services produced in response to the contract resulting from this RFP will be the sole property of the State of Colorado, unless otherwise noted in the RFP. The contents of the successful Contractor's proposal will become contractual obligations.

2. The State of Colorado has the right to retain the original proposal and other RFP response materials for its files. As such, the State of Colorado may retain or dispose of all copies as is lawfully deemed appropriate. Proposal materials may be reviewed by any person after the "Notice of Intent to Make an Award" letter(s) has/have been issued, subject to the terms of Section 24-72-201 et seq., C.R.S., as amended, Public (Open) Records. The State of Colorado has the right to use any or all information/material presented in reply to the RFP, subject to limitations outlined in the clause, Proprietary/Confidential Information. Contractor expressly agrees that the State may use the materials for all lawful State purposes, including the right to reproduce copies of the

material submitted for purposes of evaluation, and to make the information available to the public in accordance with the provisions of the Public Records Act.

1.18 INCURRING COSTS: The State of Colorado is not liable for any cost incurred by Contractors prior to issuance of a legally executed contract document. No property interest of any nature shall occur until a contract is awarded and signed by all concerned parties.

1.19 PROPOSAL REJECTION: CDOS reserves the right to reject any or all proposals and to 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 State of Colorado.

1.20 VENDOR IDENTIFICATION: The tax identification number provided must be that of the Contractor responding to the RFP. The Contractor must be a legal entity with the legal right to contract. The Contractor awarded a contract as a result of this RFP must also be registered and in good standing to do business in the State of Colorado prior to the execution of the contract.

1.21 NEWS RELEASES: News releases pertaining to this RFP shall NOT be made prior to execution of the contract without prior written approval by the State.

1.22 CERTIFICATION OF INDEPENDENT PRICE DETERMINATION:

1. By submission of this proposal each Contractor 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 Contractor 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 Contractor and will not knowingly be disclosed by the Contractor prior to opening, directly or indirectly to any other Contractor or to any competitor; and
    (c) No attempt has been made or will be made by the Contractor to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

2. Each person signing the Request for Proposal Signature Page of this proposal certifies that:
    (a) She/he is the person in the Contractor's organization responsible within that organization for the decision as to the prices being offered herein and that she/he has not participated, and will not participate, in any action contrary to (1)(a) through (1)(c) above; or she/he is not the person in the Contractor's organization responsible within that organization for the decision as to the prices being offered herein but that she/he 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 (1)(a) through (1)(c) above, and as their agent does hereby so certify; and she/he has not participated, and will not participate, in any action contrary to (1)(a) through (1)(c) above.

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

1.23 CONFLICTS OF INTEREST: The holding of public office or employment is a public trust. A public officer or employee whose conduct departs from his fiduciary duty is liable to the people of the State. Rules of conduct for public officers and state employees:

1. Proof beyond a reasonable doubt of commission of any act enumerated in this section is proof that the actor has breached her/his fiduciary duty.

2. A public officer or a state employee shall not:
   (a) Engage in a substantial financial transaction for her/his private business purposes with a person whom she/he inspects, regulates, or supervises in the course of her/his official duties;
   (b) Assist any person for a fee or other compensation in obtaining any contract, claim, license, or other economic benefit from her/his agency;
   (c) Assist any person for a contingent fee in obtaining any contract, claim, license, or other economic benefit from any state agency;
   (d) Perform an official act directly and substantially affecting its economic benefit a business or other undertaking in which she/he either has a substantial financial interest or is engaged as counsel, consultant, representative, or agent;
   (e) Serve on the Board of any entity without disclosure to the entity, the Secretary of State, and his/her employer.

3. A head of a principal department or a member of a quasi-judicial or rule-making agency may perform an official act notwithstanding paragraph (d) of subsection (2) of this section if her/his participation is necessary to the administration of a statute and if she/he complies with the voluntary disclosure procedures under C.R.S. 24-18-110.

4. Paragraph (c) of subsection (2) of this section does not apply to a member of a board, commission, council, or committee if she/he complies with the voluntary disclosure procedures under C.R.S. 24-18-110 and if she/he is not a full-time state employee.

Reference C.R.S. 24-18-108, as amended.

1.24 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 use taxes C.R.S. 39-26-114(a). The Colorado State and Local Sales Tax Exemption Number is 98-02565. Vendor is hereby notified that when materials are purchased in certain political sub-divisions (for example - City 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.

1.25 STRUCTURE OF THE RFP:

Table of Contents

1.26 Key Dates

	Activity	Deadline
1.	RFP Notice Published On the Secretary of State's website	**2/22/18**
2.	Prospective Contractors Written Inquiry Deadline (No Questions Accepted After This Date/Time)	**3/8/18 3:00 pm MST**
3.	Written Answers Provided For All Written Inquiries	**3/15/18 5:00 pm MDT**
4.	Proposal Submission Deadline Submit one original hardcopy of the Proposal marked "Original," **Five additional hardcopies** and **one copy** electronic submission **on a flash drive.**	**3/29/18 11:00 am MDT**
5.	Bid Opening	**3/29/18 11:30 am MDT**
6.	Notice of Intent to Award (estimated)	**4/19/18**
7.	Contract Period	**5/10/18 – 5/30/2019**

1.27 Definitions

Audit center – Page on the Secretary of State's website with information about the audit of the 2017 coordinated election. The page is at https://www.sos.state.co.us/pubs/elections/auditCenter.html.

Ballot contest – A partisan or nonpartisan candidate race, or a ballot measure, that appears on the ballot for an election in a county.

Ballot Manifest – A document created independently of the voting system to track the number of ballots in the election and describe how ballots are organized and stored.

Ballot polling audit – A risk-limiting audit conducted by jurisdictions using legacy systems that are not capable of exporting ballot-level cast vote records. In this audit, human beings simply report the markings on randomly selected ballots until the risk limit is satisfied.

Budget - The budget for the Work described in this RFP and its Exhibits.

Business Interruption - Any event that disrupts Contractor's ability to complete the Work for a period of time, and may include, but is not limited to a Disaster, power outage, strike, loss of necessary personnel, or computer virus.

Cast Vote Record (CVR) – An export of data from the voting system showing how the voting system interpreted the markings on every ballot scanned.

Comparison audit – A risk-limiting audit in which humans compare voter markings on randomly selected paper ballots to ballot-level cast vote records, or data showing how the voting system interpreted the markings on each individual ballot.

Coordinated election – An election occurring on the first Tuesday of November in odd-numbered years. If the Secretary of State certifies a statewide ballot measure, every county will conduct a coordinated election. Local political subdivisions may also coordinate with the county.

County administrator – The designated representative of each county clerk and recorder who possesses the RLA administrator user privileges sufficient to upload a CVR file and ballot manifest for the county.

Contest name – The title of a ballot contest.

Deliverable - The outcome to be achieved or output to be provided, in the form of a tangible or intangible object that is produced as a result of Contractor's Work that is intended to be delivered to the State by Contractor. Examples of Deliverables include, but are not limited to, report(s), document(s), server upgrade(s), software license(s), and may be composed of multiple smaller deliverables.

Disaster - An event that makes it impossible for Contractor to perform the Work out of its regular facility or facilities, and may include, but is not limited to, natural disasters, fire or terrorist attacks.

CDOS – The Colorado Department of State

Election Day – The day mandated by Colorado law for conducting a coordinated, state primary, presidential primary, or general election.

General election – An election held on the first Tuesday after the first Monday in November of even-numbered years.

Evaluation - The process of examining Contractor's Work and rating it based on criteria established in this RFP.

Fiscal Year - The State's fiscal year, which begins on July 1 of each calendar year and ends on June 30 of the following calendar year.

Goods - Tangible material acquired, produced, or delivered by Contractor either separately or in conjunction with the Services Contractor renders hereunder.

Incident - An accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State pursuant to CRS § 24-37.5-401 et seq. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a State system or State Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent.

Key Personnel - The position or positions that are specifically designated as such in this Contract.

Presidential primary election – An election conducted in a year in which a Presidential election will be held, to allocate delegates to national nominating conventions to the major political parties.

Pseudo-random number generator – A random number generator application that is further explained at http://statistics.berkeley.edu/~stark/Java/Html/sha256Rand.htm.

Risk-limiting audit (RLA) – An audit that provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.

Random seed – A number (or vector) used to initialize a pseudo-random number generator.

Risk Limit – The largest chance that a wrong outcome will not be corrected.

RLA Artifacts – The artifacts relating to the initial RLA code for the State, available at the following link: https://github.com/FreeAndFair/ColoradoRLA

Services - The required services to be performed by Contractor pursuant to this RFP.

State administrator – The designated representative of the Secretary of State, who possesses RLA administrator user privileges to perform administrative tasks.

State Controller - The Colorado State Controller or authorized designee of the Colorado State Controller.

State Information - The combination of State Confidential Information and State Records.

State primary election – An election held on the last Tuesday of June in even-numbered years in which candidates are nominated to the general election ballot for participating parties.

State Records – All information, data, records, and documentary materials which are not sensitive and belong to the State regardless of physical form or characteristics, including but not limited to any public State records, non-sensitive State data, and other information or data concerning individuals that is not deemed confidential but nevertheless belongs to the State, which has been communicated, furnished, or disclosed by the State to Contractor which (i) is subject to disclosure pursuant to the Colorado Open Records Act, CRS § 24-72-200.1, et seq.; (ii) is already known to Contractor without restrictions at the time of its disclosure by Contractor; (iii) is or subsequently becomes publicly available without breach of any obligation owed by Contractor to the State; (iv) is disclosed to Contractor, without confidentiality obligations, by a third party who has the right to disclose such information; or (iv) was independently developed without reliance on any State Confidential Information. Notwithstanding the foregoing, State Records shall not include State Confidential Information.

Subcontractor – Any third party engaged by Contractor to aid in performance of Contractor's obligations.

Tabulated ballots – Paper ballots that have been scanned on a ballot scanning device, and the voters' markings on which have been interpreted by the voting system's software as valid votes, undervotes, or overvotes.

Two-factor authentication – Defined as two out of the three following requirements:

- Something you have (i.e., Token code)
- Something you know (i.e., password)
- Something you are (i.e., biometrics. Examples include finger print scan, etc.)

Work – The tasks and activities Contractor is required to perform to fulfill its obligations under this RFP and its Exhibits, including the performance of the Services and delivery of the Goods.

Work Product - The tangible or intangible results of Contractor's Work, including, but not limited to, software, research, reports, studies, data, photographs, negatives, or other finished or unfinished documents, drawings, models, surveys, maps, materials, or work product of any type, including drafts.

Wrong outcome – When the reported outcome does not match the actual outcome (i.e., the wrong candidate was reported as the winner).

Section 2: RLA Background and Overview

2.1 RLA BACKGROUND AND OVERVIEW:

Beginning with the November 7, 2017, coordinated election, Colorado counties are required by law to conduct a new post-election audit called a risk-limiting audit following each coordinated, primary, and general election (Section 1-7-515, C.R.S.). The Secretary of State promulgated administrative rules governing the manner in which the counties conducted the audits (Election Rule 25). In adopting the rules, the Secretary of State consulted experts and county clerks.

Following adoption of the rules, the Secretary of State contracted with Free & Fair to develop a software tool for implementation in the 2017 coordinated election audit. The purpose of the software tool was to make the audit as effective and efficient as possible for the county in conducting the audit and the state in administering the audit.

In the 2017 coordinated election, 50 counties using a new voting system capable of exporting a ballot-level cast vote record used the software tool conduct a comparison risk-limiting audit of the election.

Section 3: Statement of Work

3.1 DELIVERABLE #1: PHASE II DEVELOPMENT REQUIREMENTS

3.1.1 Contractor must meet all of the Phase II Development Requirements as outlined in **Exhibit A.**

3.2 DELIVERABLE #2: PHASE II SYSTEM REQUIREMENTS

3.2.1 Contractor must meet all of the Phase II System Requirements as outlined in **Exhibit D**.

3.3 DELIVERABLE #3: DEVELOPMENT PLAN

3.3.1 Onsite planning sessions between the Contractor and CDOS. During the session the Contractor shall develop, with the state's input, a development plan that shall include, at a minimum: Overall plan of operation, including all deliverable dates and state indicated deadlines.

Section 4: Contractor Response

The purpose of this RFP is to select a Contractor to develop enhancements to the risk-limiting audit software system. All Contractors must respond to this Section, starting with paragraph 4.1 of this RFP. Contractors shall respond to each paragraph and subparagraph of the section using the same numbering system.

4.1 GENERAL INFORMATION AND COMPANY OVERVIEW

The Contractor shall complete the Request for Proposal Cover/Signature Page which provides necessary company and point of contact information. This must be included with the Contractor response.

4.1.1 COMPANY HISTORY

The Contractor shall provide the number of years established and a short history of business offerings specific to providing operational hosting and support solutions.

4.1.2 ORGANIZATIONAL STRUCTURE

Describe the organizational structure for the Contractor. This should include the total number of employees as well as the number and geographic location of offices.

4.1.3 FAILURE TO COMPLETE

Disclose whether the Contractor (or any general partner or joint venture of the Contractor) has failed to complete a similar project within the past five years. If so, list the date of commencement of the project and the entity for which the project was to be performed, and explain why the project was not completed.

4.1.5 CONFLICT OF INTEREST

The Contractor shall document any conflict(s) of interest due to any other clients, contracts, or property interest.

4.1.6 DISCLOSURE OF OUTSTANDING LITIGATION

Explain in detail whether the Contractor's company is currently part of or has been part of any litigation related to implementing a software system within the past five years.

4.2 SUMMARY OF QUALIFICATIONS

CDOS requires the Contractor to have superior capability and experience in software development. The Contractor shall provide client references for three relevant qualifications that demonstrate proven experience developng and deploying a software system for a mission-critical public or commercial sector business application. Please provide a direct reference for each qualification. Specifically, qualifications should validate each of the following key areas (Note: Contractors may elect to use individual qualifications to meet each of the following below):

- Demonstrated experience of same size and scope
- Demonstrated ability to meet stringent government security requirements such as those outlined in Exhibit B.

Finally, each of these qualifications must describe the business scenario and a brief description of the approach and an overview of operational support services provided. Contractors should provide a narrative on providing local on-site support for the environment.

4.3 REFERENCES

The Contractor shall provide references for each qualification requested in Section 4.2 and may also elect to provide up to three additional references from current and/or past customers for the last three years, of comparable size and scope, who can attest to the Contractor's experience and qualifications as it relates to the scope of the work described above. Each reference must include the following information:

1. Client Name
2. Project Name
3. Contact Name
4. Contact Title
5. Contact Phone Number
6. Contact Email Address

CDOS reserves the right to independently identify and contact other references in addition to those listed above.

4.4 TECHNICAL RESPONSE TO REQUIREMENTS

In order to effectively and efficiently validate requirements, the Contractor must provide a narrative on how it meets the CDOS requirements outlined in Section 3 – Statement of Work in the order outlined in bullet points below. Narrative should be no more than 15 pages in length.

- Provide documentation demonstrating how the system meets the minimum security requirements outlined in Exhibit B, including completion of the checklist provided in Exhibit C.

- Provide milestones and development timelines required by the development requirements outlined in Exhibit A.

- Provide documentation demonstrating how the proposed system meets the core requirements outlined in Exhbit D.

- Provide a project plan for development and testing.

- Provide audited financial statements for the two most recently completed years, and a pro forma balance sheet and income statement for the current year, demonstrating financial solvency and stability.

4.6 PROJECT MANAGEMENT AND GOVERNANCE

The Contractor shall provide a brief summary of its management and escalation processes, including:

- Providing effective communication with the CDOS Management Team.
- Managing changes to contract scope and service level agreements.
- Managing issues and risks.
- Ensuring quality control.

4.7 PROPOSED STAFFING

The Contractor shall provide the following in terms of staffing:

1. Project organization chart that should identify necessary involvement from CDOS staff.
2. Itemization of all staff, consultants and subcontractors to be used by the Contractor on this project. Briefly outline the responsibilities for each of these resources. (Please note that background checks will be required for all personnel who will be used on this project. In addition, such personnel may be required to sign statements of non-disclosure of confidential information.)
3. Identification of the local support resource(s).
4. Staff, consultant or subcontractor biographies which should provide the following:
    (a) Name
    (b) Title
    (c) Project Role
    (d) Percentage of time dedicated to the project
    (e) Brief Summary of work experience and/or qualifications
5. Resumes should be provided as an appendix for all proposed staff.

4.8 FACILITY AND OTHER REQUIREMENTS

Provide a clear description of any facility, personnel, and other requirements needed for the accomplishment of the project that CDOS will be expected to provide.

CDOS reserves the right to provide only those facilities, personnel, and other requirements as CDOS deems necessary and appropriate.

4.9 WORKING ASSUMPTIONS

The Contractor shall identify and list specific working assumptions used in the approach, cost and project schedule.

4.12 FINANCIAL CONSIDERATIONS

The Contractor shall provide detailed cost estimates and proposed payment schedule including fees and expenses for the project. Please provide unit based costing for the following contractual components:

- Transition Planning and Execution
- Architectural Assessment
- Operations Support (Monthly Cost)

Section 5: Proposal Instructions, Evaluation, and Award

5.1 SUBMISSION AND GENERAL INSTRUCTIONS

Proposals must be received on or before the date and time indicated in the Schedule of Activities. It is the responsibility of the Contractor to ensure that the proposal is received on or before the proposal due date and time, regardless of the delivery method used.

Section 4.0 shall be considered the response starting point and Contractors shall have their responses starting at Section 4.1.

CDOS emphasizes Contractors are to respond with their best proposal for this RFP. If there are requirements which seem unreasonable or if better concepts or practices are available to CDOS, the Contractor should provide them.

Submit one original and five copies of the proposal, as well as an electric copy on a flash drive in Word or Adobe Acrobat PDF format. Cost proposals must be separate from the technical response. The proposal package shall be delivered or sent by mail to:

Attn: Brad Lang
Controller & Budget Director
Colorado Department of State
1700 Broadway, Suite 200
Denver, CO 80290

Address written inquiries to: Brad.Lang@sos.state.co.us (**Proposals must NOT be emailed**)

The proposal must be signed in ink by an officer of the Contractor who is legally authorized to bind the Contractor to the proposal. Proposals which are determined to be at a variance with this requirement may not be accepted. A proposal signature page has been provided with this RFP. Proposals must be submitted and sealed in a package with an appropriate label affixed. The label must show the following information:

<Contractor's Name>
RFP CDOS-Elections-RFP-2018-001
Proposal Due March 29, 2018 at 11:00am. MDT

CDOS desires and encourages that proposals 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, as well as the use of unnecessarily elaborate proposals, is discouraged.

5.2 PROCESS

A review committee will evaluate the merits of proposals received in accordance with the evaluation factors stated in this RFP and formulate a recommendation.

Failure of the Contractor to provide all the information requested in this RFP may result in disqualification of the proposal. This responsibility belongs to the Contractor.

The sole objective of the review committee will be to recommend the Contractor whose proposal is most responsive to the State's needs while charging reasonable transactional fees. The specifications within this RFP represent the minimum performance necessary for response.

5.3 EVALUATION FACTORS

All proposals submitted in response to this RFP will be evaluated by a committee of CDOS personnel.

The Evaluation Committee will judge the merit of proposals received in accordance with the criteria described below (in no particular order):

(a) **Development requirements**
(b) **System requirements**
(c) **System security**
(d) **Outline of milestones and development timeline**
(e) **Proposed project plan**
(f) **Vendor's financial stability**
(g) **Documented experience**
(h) **Overall cost and proposed payment schedule**

Section 6: Exhibits

Exhbit A – Risk-Limiting Audit Software: Phase II Development Requirements (and Attachment)
Exhibit B – Security Standards
Exhibit C – Security Requirements Checklist
Exhibit D – Risk-limiting Audit Core System Requirements

Exhibit A

Risk-Limiting Audit Software: Phase II Development Requirements

Table of Contents

Purpose and Audience

The purpose of this document is to outline in detail the requirements for additional development of the Colorado Risk-Limiting Audit (RLA) software, to support statistically valid RLAs of statewide, multi-county, and single-county ballot contests in primary, coordinated, general, congressional vacancy elections, and other local elections. This document is targeted to anyone involved in the project.

Vision

"[Risk-limiting audits are] an important step in assuring people that the votes that were cast were counted accurately and reported accurately. People need to have confidence in the elections process; it is the basis of the democratic republic in which we live. And so it plays a critical role in providing that assurance to every Coloradan and frankly every American that our elections are run well here in the state of Colorado." - Colorado Secretary of State Wayne Williams

System Background

Business Context

Colorado law requires the Secretary of State to implement risk-limiting post-election audits following each primary, general, coordinated, and congressional vacancy election, and to adopt administrative rules prescribing the manner in which RLAs must be conducted (section 1-7-515, C.R.S. (2017))[1]. In 2017, the Secretary of State adopted Election Rule 25[2], requiring the Secretary of State to administer, and counties to conduct, the risk-limiting audits. Currently, counties that use voting systems capable of capturing and exporting ballot-level cast vote records must perform a type of RLA called a comparison audit. Under the Election Rules, the Secretary of State selects as the audited contests at least one statewide contest, and for each county at least one countywide contest (Election Rule 25.2.2(i)). The Secretary of State selects other ballot contests for audit if in any particular election there is no statewide contest or no countywide contest in any county.

[1] The 2017 version of Title 1 of the Colorado Revised Statutes is available online at http://www.sos.state.co.us/pubs/elections/LawsRules/files/Title1.pdf

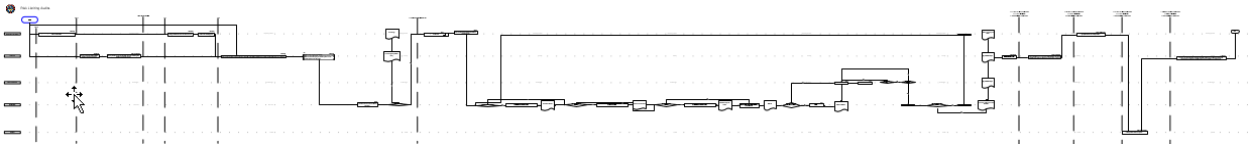
[2] The current version of the Election Rules, 8 CCR 1505-1, were adopted on 12/07/2017, and are available at https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1Elections.html

Stakeholders

Stakeholder	Title	Interests and Needs
Wayne Williams	Secretary of State	Providing assurance to the public of a well-run election
Judd Choate	Director Of Elections	Executive Sponsor
Trevor Timmons	Chief Information Officer	Technical Support
Hilary Rudy	Deputy Elections Director	Legal Compliance
Dwight Shellman	County Support Manager	Ease of use by the counties
Jessi Romero	Voting Systems Manager	Functional testing and state audit administrator
Danny Casias	Senior Voting Systems Specialist	Functional testing and state audit administrator
County audit administrators		Upload data necessary for state to define and commence RLA; launch user interface for county audit boards
Audit boards		Bipartisan county teams that locate and retrieve randomly selected ballots from storage locations, and report voter markings from those ballots into RLA software

System Context

See Appendix A for detailed view and embedded flow diagram



.

Statistical Concepts

Risk-limiting audits provide a statistical level of confidence that the outcome of the election is correct, and limits the risk that a jurisdiction will certify an incorrect election outcome. For example, if the risk limit for the audit is 10%, then there is at least a 90% probability that the audit will discover and correct a wrong outcome if one exists; And at most a 10% chance that the audit will not discover an incorrect outcome.

In a comparison audit, individual ballot cards are randomly selected from all ballots cast in the election. Each selected ballot is then manually interpreted and that interpretation is checked against the electronic record of the selected ballot. Once a statistically significant number of ballots have confirmed the stated election results, the audit can stop. The audit must continue until the risk limit is met or a full hand count occurs.

For further information about RLAs, please review the published materials available on the Secretary of State's website at https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditResources.html.

Minimum Viable Product

All Elections

The current version of the Colorado RLA software, developed by Free and Fair in 2017[3], supports RLAs of ballot contests within individual counties. The next version of the software must support a statistically valid RLA for a statewide ballot contest shared by all counties (e.g., a statewide ballot measure), or ballot contests shared by some but not all counties (e.g., Congressional and state legislative candidate contests).

The Secretary of State may also make the RLA software available to the designated election officials of other types of political subdivisions to conduct RLAs of one or more different elections that occur on the same or different days throughout the calendar year. Ideally, the RLA software should be capable of hosting and independently administering RLAs of different elections on the same or different days. The following are the necessary functions for conducting the audit using the software.

Before the onset of the audit, each county audit administrator will upload a cast vote record (CVR) file, a ballot manifest file, and file hash values. The software should verify that the number of ballot cards reflected in each county's CVR file matches the number of ballot cards reflected in the county's ballot manifest. If the numbers do not match, the software should notify the state and county audit administrators of the issue.

The software must be able to identify the jurisdictional nature of all ballot contests in each county's CVR file:

- Contests shared by all counties (statewide),
- Contest(s) shared by more than one county (multi-county), and
- Contest(s) that are strictly within a single county (single-county).

In addition, the system must be able to accurately identify and match each county's variation of the contest name with the standardized name of the contest in the system. The state audit administrator will need a screen from which to map any unidentified column(s) to the contest(s).

The state must have the ability to specify as audited contests one or more statewide, multi-county, and single-county ballot contests.

For each type of statewide or single-county audited contest, the one with the smallest diluted margin will determine the number of ballots to be randomly selected. Each multi-county audited contest must be evaluated separately.

The software must also randomly select ballots from the universe of total ballots cast that corresponds to the nature of the audited contest.

Once the software determines the number of ballots that must be examined to satisfy the risk limit for all audited contests, and randomly selects that number of ballots from the appropriate universe of

[3] For more information on the software as it exists in its current state, please see the materials posted in the GitHub repository, available at https://GitHub.com/FreeAndFair/ColoradoRLA.

ballots cast, the system must compile a ballot list for each county that contains all ballots randomly selected for all statewide, multi-county and single-county audited contests in that county, with any duplicate ballot cards removed.

The current version of the software permits a single bipartisan county audit board to report votes from the ballots randomly selected for audit in that county. A county that is required to audit a large number of ballot cards needs the ability to have multiple county audit boards working in the software simultaneously. The next version of the software must provide a way for each county audit administrator to specify the number of audit boards at the time he or she uploads the county's ballot manifest and CVR file. The software must also evenly divide the county's ballot list amongst the county's individual audit boards. The ballot list should be sorted in ascending order by device ID – batch no. – ballot position no.

Utilizing the random seed, the random selection of ballots should come from the ballot manifests, not the CVRs. When selecting the ballots for auditing on a multi-county or statewide level, the software should compile individual county ballot manifests into a single ballot manifest from which to randomly select the ballots. The system should distribute the list of randomly selected ballots to the counties, with information to allow the county to identify the ballots to be audited.

The current software-guided process of how the audit board enters its interpretation of the ballots can continue to function, as it currently exists. When the audit board examines a single ballot, it will enter its interpretation into the software the votes in all contests on the selected ballot card.

Once a county audit board has individually submitted its report of voter markings on each randomly selected ballot in its ballot list, the software should provide the audit board with a final opportunity to review all ballot markings reported for all ballots in the audit round. The county audit board may choose or decline to do so before final submission. The software then notifies the county audit board to wait on the other boards within their county to complete final submission. After all boards have completed final submission, the software notifies the county of their completion of the current round, and to wait on notification from the state audit administrator. Once all counties have completed their submission, the software should notify all county audit administrators and state audit administrators of the status of each applicable audited contest audit, and calculate whether an additional round is necessary –. If another round is required, the audited contest within a jurisdictional nature for which the risk limit was not satisfied with the smallest diluted margin will determine the number of ballots selected.

Primary Elections

In a primary election, audited contests will be selected for each party and the random selection of ballots for a particular audited contest should be limited to the ballots for that party. Diluted margin needs to be calculated based on total ballots cast in that party at the appropriated jurisdictional nature (statewide, multi-county, single-county). Once the software verifies that the total number of ballots in the ballot manifest equals the total ballots reflected in the CVR, the ballot selection must take into consideration the ballot style to ensure that the ballots selected for each audited contest are from the correct party ballot style.

Requirements Specification

Browsers

- The software must be compatible with all recent versions of major commercially available browsers, e.g., Chrome, Firefox, Safari, Internet Explorer, and Edge.

User Experience

Interested respondents should propose User Experience (UX) enhancements that address the following issues.

- The information architecture should be structured in a way that communicates to the users at a glimpse.
- Messaging needs to be clear and succinct
    - Categories of messaging include:
        - Error Messages
        - Task Messages
        - Status Messages
            - The audit completion message should be particular noteworthy
        - Next Steps Messages
        - Warning messages before allowing execution of critical functions

Software Modifications

Logging in

- When entering the three grid values for two-factor authentication, a county audit administrator must be able to enter the values sequentially instead of having to use the tab key or mouse to select three different fields.

Ballot manifest file upload

- The tabulator ID field of the ballot manifest needs to be modified to accept text strings.

CVR file upload

- Optimize upload process by minimizing the amount of in-transit data parsing.
- Accept CVR files generated by the Clear Ballot Group's ClearVote 1.4.1 voting system and Dominion Voting Systems' Democracy Suite 5.2 voting system.
- The information that appears in each voting system's CVR file is not necessarily in the same column/row location so the software will need to be able to distinguish which type of CVR has been uploaded and to extract the appropriate information from the correct location.

Cast Vote Record

Dominion

- The cast vote records start in row 5

Clear Ballot

- The cast vote records start in row 2

Ballot headers

Ballot header information contains data enabling counties to locate and retrieve specific ballot cards.

Dominion

- The ballot header information for the Dominion CVR begin at row 4. The first seven columns shown below are an example format of an uploaded Dominion CVR.

	A	B	C	D	E	F	G
1	County Coordi	5.2.16.1					
2							
3							
4	CvrNumber	TabulatorNum	BatchId	RecordId	ImprintedId	PrecinctPortion	BallotType
5	1	5	1	1	5/1/2001	6273703281 (281-44)	44
6	2	5	1	2	5/1/2002	6295603329 (329-51)	51

Clear Ballot

- The first 10 columns of the Clear Ballot CVR contain ballot header information. Clear Ballot uses batch header sheets to define the ballot groups (e.g., AB for absentee ballots, ED for election day) and batch number. The 10 columns shown below are an example format of an uploaded Clear Ballot CVR.

	A	B	C	D	E	F	G	H	I	J
1	RowNumber	BoxID	BoxPosition	BallotID	PrecinctID	BallotStyleID	PrecinctStyleName	ScanComputerName	Status	Remade
2	1	AB-4067826	1	AB-4067826+10001	3	1	01 Standa	GEMY513001WA	0	0
3	2	AB-4067826	2	AB-4067826+10003	3	1	01 Standa	GEMY513001WA	0	0

- When mapping a Clear Ballot to Dominion CVRs for ballot location information:
    - Clear Ballot's BoxID = Dominion's BatchID
    - Clear Ballot's BoxPosition = Dominion's RecordID
    - Clear Ballot's CVR does not contain a field corresponding to Dominion's TabulatorNum field. For counties using the Clear Ballot system, the ballot list generated by the software should contain null values in the TabulatorNum field.

Contest headers

Dominion

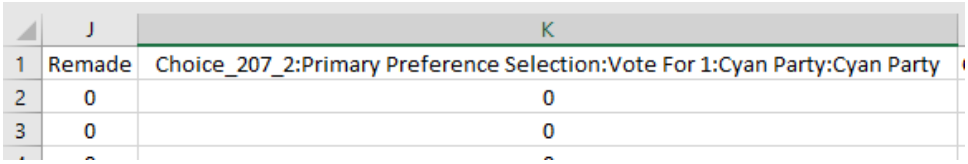
- The Dominion system identifies ballot contests in the top 4 rows of the CVR. The contest name and "vote for" information appears in a field in row 2, the choice name appears in a field in row 3, and a candidate's party is in a filed in row 4.

	G	H
1		
2		United States Senator - DEM (Vote For=1)
3		Michael Bennet
4	BallotType	DEM
5	District Style 2	
6	District Style 2	

Clear Ballot

- The Clear Ballot system identifies ballot contests in the first row of each column of the CVR applicable to a contest. The following parameters are included and separated by a colon.
    - Choice_X_X, where X_X equals <Choice ID>_<PartyID>
    - <ContestName>
    - <VoteRule>
    - <ChoiceName>
    - <PartyName>

  The contest name, vote for, and choice names need to be extracted from each contest header.



	J	K
1	Remade	Choice_207_2:Primary Preference Selection:Vote For 1:Cyan Party:Cyan Party
2	0	0
3	0	0

Audit Definition

- The RLA software must enable the Secretary of State to select one or more statewide, multi-county and single-county ballot contests as the audited contests in the RLA.
    - The software must randomly select ballots from the ballot manifest and not the CVR.
    - The software must compile a single ballot list for each county containing all ballots cast in that county that were randomly selected for all audited contests. For each randomly selected ballot, the ballot list must include the tabulator ID (if applicable), batch ID, position within the batch, and storage location
    - Assigning the correct ballots to the correct county for auditing.
    - The software must identify the jurisdictional nature of and associate all ballot contests as statewide, multi-county or single-county, in all CVR files uploaded by all counties. This may require the software to identify and associate contest or candidate names that are not exactly identical in every county's CVR (e.g., "Secretary of State" vs. "State Secretary"). When the software is unable to correctly correlate a CVR contest header with a known contest, the state administrator must have the ability to map the statewide and multi-jurisdictional contests from the state administrator pages.
- The software should display the applicable voting choices when the state audit administrator uses a mouse to "hover" over the ballot contest name when selecting audited contests
- After the state audit administrator has defined the audit by entering the risk limit(s), random seed, and selecting the audited contests, the software should display a review screen showing all audited contests and the number of ballots that must be audited in each affected county. The state audit administrator should be able to commence the audit from the review page, or revise elements of the audit's definition. The software should support exporting the information displayed on the review screen as a report.

Ballot Assignment

- The software should make available for download each county's ballot list in csv format on the county administrator's landing page.
    a. The ballot list should contain the following information about each ballot to be audited:
        i. Tabulator ID (if applicable)
        ii. Batch
        iii. Ballot position
        iv. Location
        v. County name
    b. In the case of multiple audit boards within a county:
        i. The software must provide a way for the county audit administrator to specify the number of audit boards
        ii. The software must include on the county audit administrators' landing page a downloadable single ballot list and a ballot list for each audit board. The ballot lists for each audit board should identify the audit board for which they are intended.
        iii. The ballot list should contain an additional field: Audit Board
        iv. Divide the single ballot list amongst the boards evenly
        v. The batch(s) and bin(s) contained in the list should be divided in a logical manner.

Audit Status

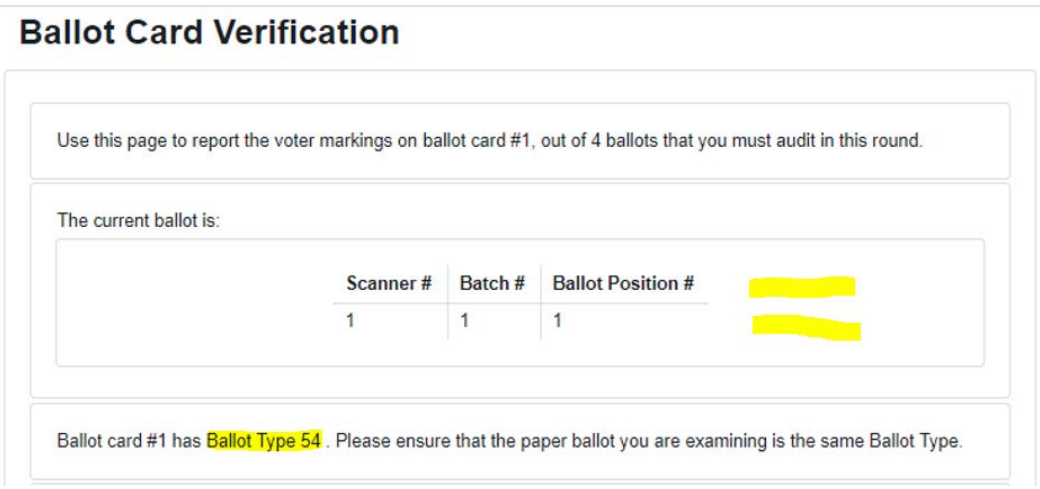
- If a county had multiple contests at the same or different levels (statewide, multi-county, county) being audited, the software should allow the state audit administrator to terminate:
    - The audit of one contest while allowing for the continued audit of other contests.
    - A contest for one county while other counties continue to audit that contest. In this case the county's audit status should be listed as "Partially terminated " and the aborted contest status should be listed as "Audit terminated".
    - All contests for a county while other counties continue to audit, including other counties that may share a contest with the county whose contests were terminated
- When a county's audit has been terminated by the state audit administrator, the county's status should be listed as "Audit terminated" instead of "Audit complete".

Conducting the Audit

- Change the number of discrepancies in a non-audited contest to reflect the number of discrepancies in all non-audited contests. Currently, the number of discrepancies is the

number of ballots that contain a discrepancy in any non-audited contest and not the total number of discrepancies on all non-audited contests for all ballots.

- On the ballot Card Verification screen: Add the ballot type information into the description following "The current ballot is:" (Scanner #, Batch #, Ballot Position #) of the current ballot so that it is more visible. As seen below.



- Once a county audit board has individually submitted its report of voter markings on each randomly selected ballot in their ballot list, the software should provide the audit board with a final opportunity to review all ballot markings reported for all ballots in the audit round. The county audit board may choose or decline to do so before final submission.
- The software should notify all county audit administrators that participated in the first audit round (or the most recent audit round) about the whether or not they are required to conduct a subsequent round.

Dashboards

System Users

- Each user group should have a dashboard that will serve as its home and communications page.
  - State audit administrator
    - The dashboard should reflect changes in audit status when contests are terminated
  - County audit administrator
    - The county audit administrator should be able to launch additional audit board sessions, if the county designates more than one audit board for the RLA.
  - County audit board(s)

Public

- Publicly accessible dashboard showing:
  - Status of each county on a real time basis (county z in on ballot x of y)
  - Tasks completed

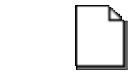
Reports

- Internal dashboard for tabular reports. The current system reports are not aesthetically or architecturally appealing. A better solution should be designed.
    - The Audit certificate Report must be available to print via PDF.

Appendices

A. Process Flow

This embedded document is also attached separately as a PDF.



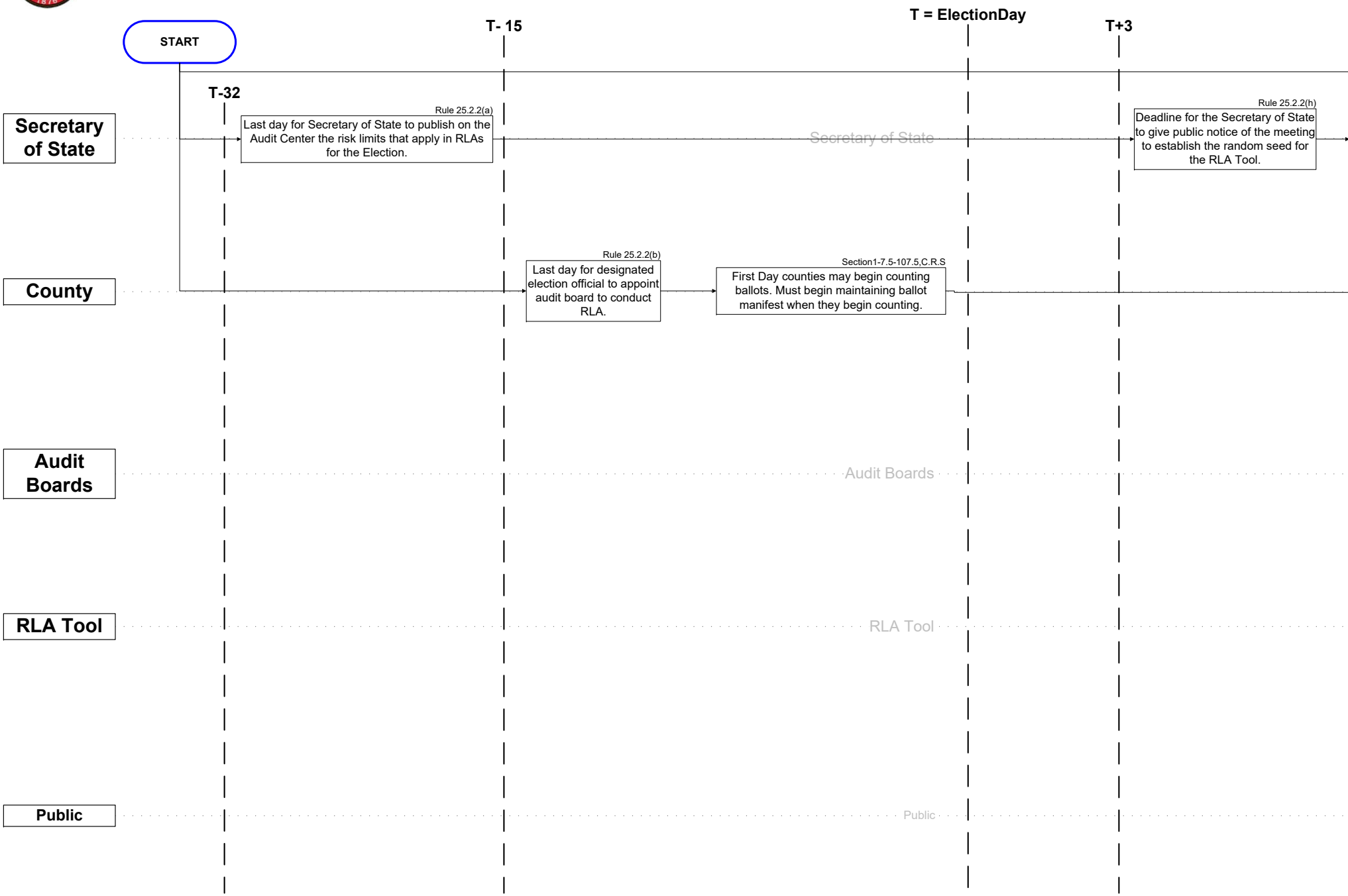
Visio-rla printable DLC.pdf

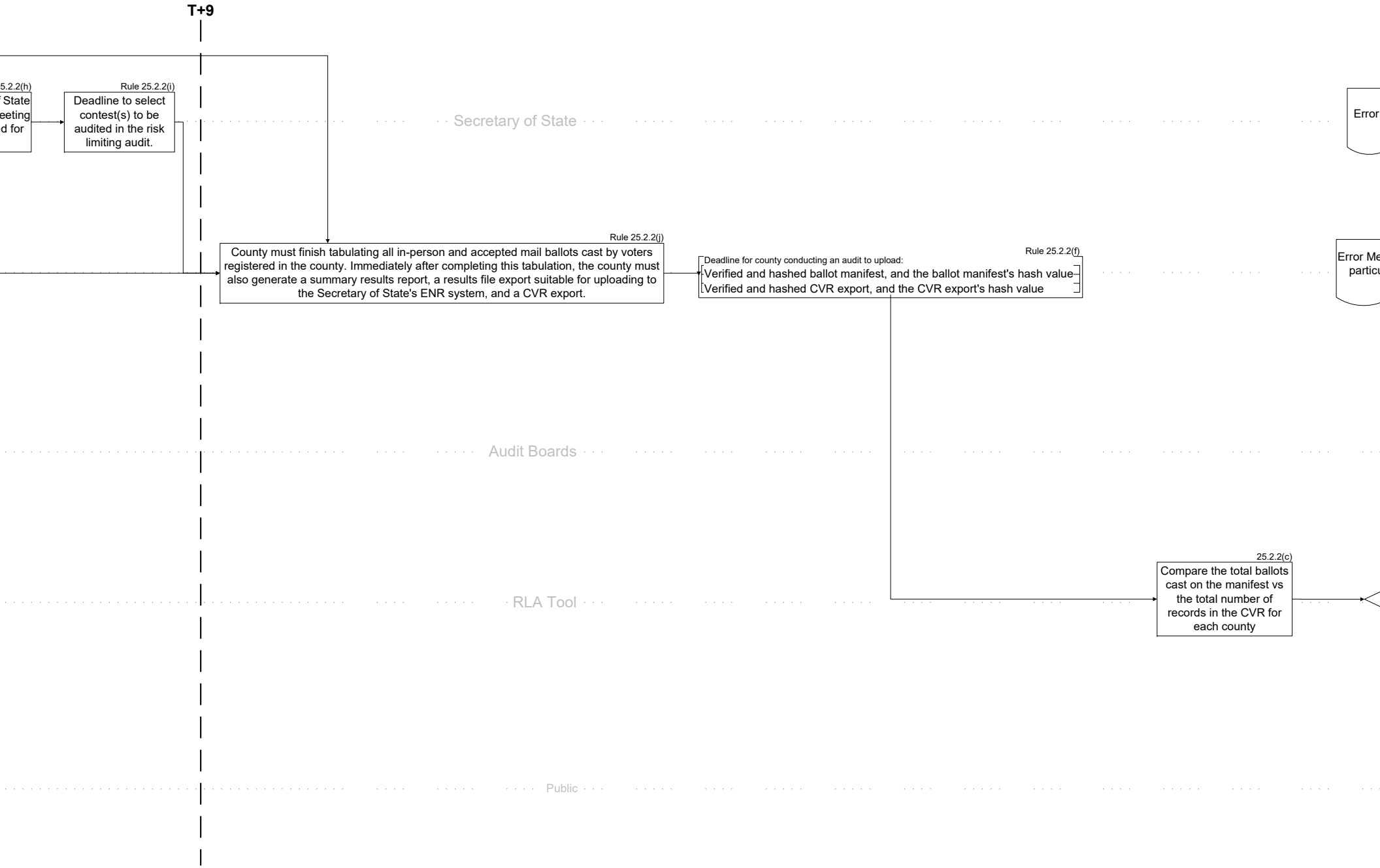
B. Glossary of Terms

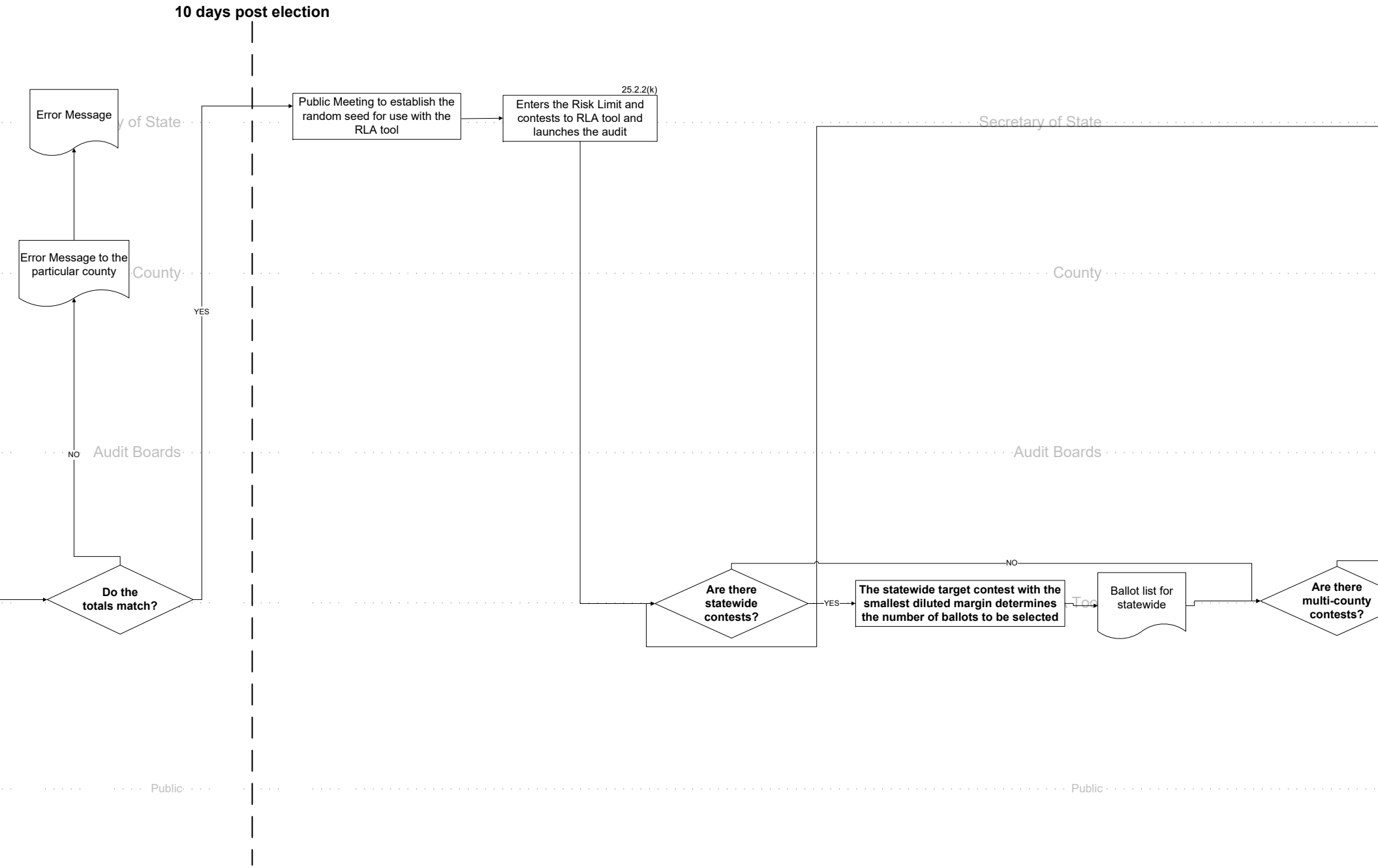
- Audit board: A pair of bipartisan election judges in a county that conducts the audit.
- Audit center: Page on the Secretary of State's website with information about the audit of the 2017 coordinated election. The page is at https://www.sos.state.co.us/pubs/elections/auditCenter.html.
- Ballot contest: a partisan or nonpartisan candidate race, or a ballot measure, that appears on the ballot for an election in a county
- Ballot manifest: A document created independently of the voting system to track the number of ballots in the election and describe how ballots are organized and stored.
- Cast Vote Record (CVR): An export of data from the voting system showing how the voting system interpreted the markings on every ballot scanned.
- Comparison audit: Risk-limiting audit in which humans compare voter markings on randomly selected paper ballots to ballot-level cast vote records, or data showing how the voting system interpreted the markings on each individual ballot.
- Coordinated election: An election occurring on the first Tuesday of November in odd-numbered years. If the Secretary of State certifies a statewide ballot measure, every county will conduct a coordinated election. Local political subdivisions may also coordinate with the county.
- County administrator: The designated representative of each county clerk and recorder who possesses the RLA administrator user privileges sufficient to upload a CVR file and ballot manifest for the county.
- Contest name: The title of a ballot contest.
- Election Day: The day mandated by Colorado law for conducting a coordinated, state primary, presidential primary, or general election.
- General election: An election held on the first Tuesday after the first Monday in November of even-numbered years.

- Presidential primary election: An election conducted in a year in which a Presidential election will be held, to allocate delegates to national nominating conventions to the major political parties.
- Pseudo-random number generator: A random number generator application that is further explained at http://statistics.berkeley.edu/~stark/Java/Html/sha256Rand.htm.
- Risk-limiting audit (RLA): An audit that provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.
- Random seed: A number (or vector) used to initialize a pseudo-random number generator.
- Risk Limit: The largest chance that a wrong outcome will not be corrected.
- RLA Artifacts: Artifacts relating to the initial RLA code for the State, available at the following link: https://github.com/FreeAndFair/ColoradoRLA
- State primary election: An election held on the last Tuesday of June in even-numbered years in which candidates are nominated to the general election ballot for participating parties.
- State audit administrator: The designated representative of the Secretary of State, who possesses RLA administrator user privileges to perform administrative tasks.
- Tabulated ballots: Paper ballots that have been scanned on a ballot scanning device, and the voters' markings on which have been interpreted by the voting system's software as valid votes, undervotes, or overvotes.
- Two-factor authentication: Defined as two out of the three following requirements:
    - Something you have (i.e., Token code)
    - Something you know (i.e., password)
    - Something you are (i.e., biometrics. Examples include finger print scan, etc.)
- Wrong outcome: When the reported outcome does not match the actual outcome (i.e., the wrong candidate was reported as the winner).

Risk Limiting Audits



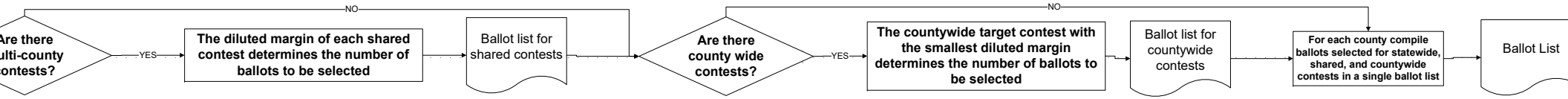

T+9
5.2.2(h)
State
eeting
d for
Rule 25.2.2(i)
Deadline to select contest(s) to be audited in the risk limiting audit.
Secretary of State
Error
Rule 25.2.2(j)
County must finish tabulating all in-person and accepted mail ballots cast by voters registered in the county. Immediately after completing this tabulation, the county must also generate a summary results report, a results file export suitable for uploading to the Secretary of State's ENR system, and a CVR export.
Rule 25.2.2(f)
Deadline for county conducting an audit to upload:
Verified and hashed ballot manifest, and the ballot manifest's hash value
Verified and hashed CVR export, and the CVR export's hash value
Error Me
particu
Audit Boards
25.2.2(c)
Compare the total ballots cast on the manifest vs the total number of records in the CVR for each county
RLA Tool
Public


10 days post election
Error Message
Public Meeting to establish the random seed for use with the RLA tool
25.2.2(k)
Enters the Risk Limit and contests to RLA tool and launches the audit
Secretary of State
Error Message to the particular county
County
YES
NO
Audit Boards
Do the totals match?
Are there statewide contests?
YES
NO
The statewide target contest with the smallest diluted margin determines the number of ballots to be selected
Ballot list for statewide
Are there multi-county contests?
Public

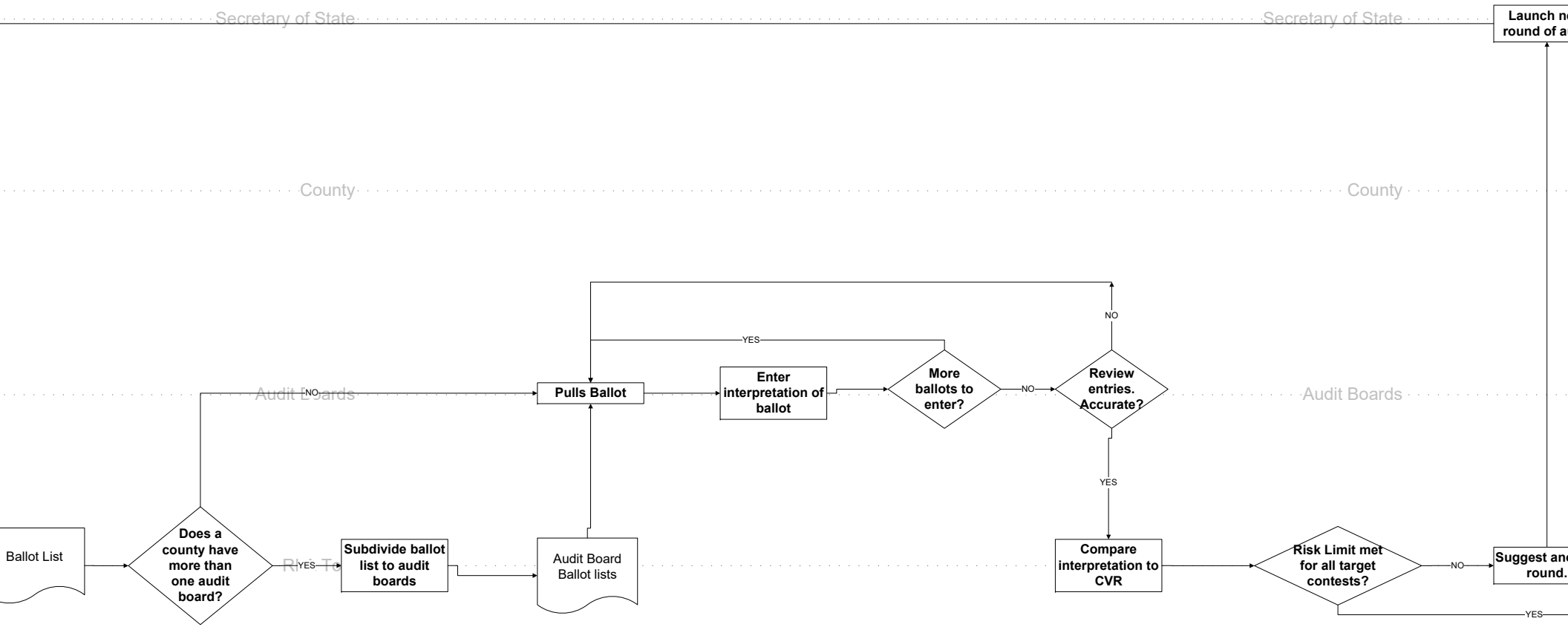
Secretary of State

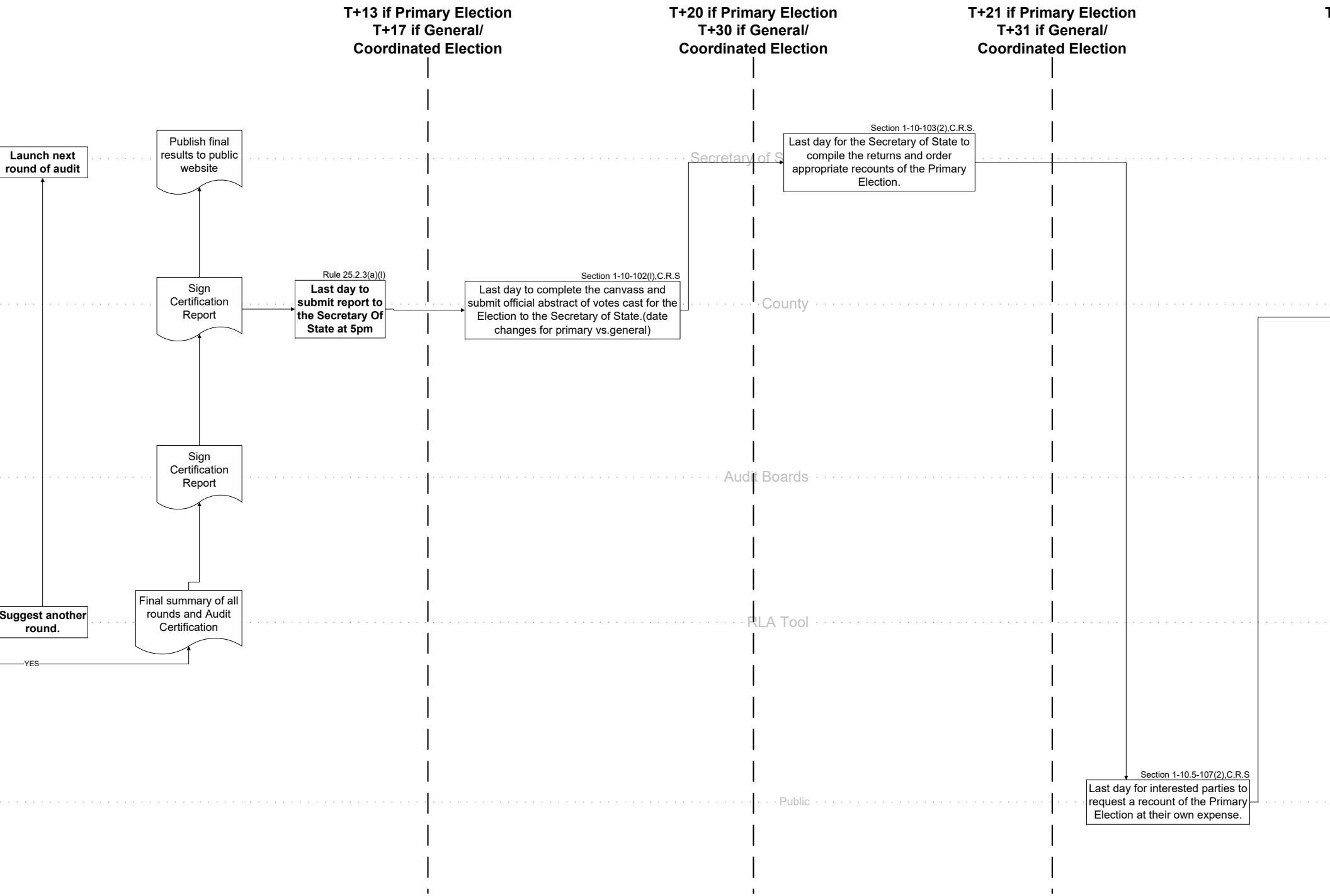
County

Audit Boards



Public


Secretary of State
Launch n
round of a
County
Audit Boards
Public
Ballot List
Does a county have more than one audit board?
YES
NO
Subdivide ballot list to audit boards
Audit Board Ballot lists
Pulls Ballot
Enter interpretation of ballot
More ballots to enter?
NO
YES
Review entries. Accurate?
NO
YES
Compare interpretation to CVR
Risk Limit met for all target contests?
NO
YES
Suggest an
round.


T+13 if Primary Election
T+17 if General/
Coordinated Election
T+20 if Primary Election
T+30 if General/
Coordinated Election
T+21 if Primary Election
T+31 if General/
Coordinated Election
Launch next round of audit
Publish final results to public website
Section 1-10-103(2),C.R.S.
Last day for the Secretary of State to compile the returns and order appropriate recounts of the Primary Election.
Secretary of S
Sign Certification Report
Rule 25.2.3(a)(I)
Last day to submit report to the Secretary Of State at 5pm
Section 1-10-102(I),C.R.S
Last day to complete the canvass and submit official abstract of votes cast for the Election to the Secretary of State.(date changes for primary vs.general)
County
Sign Certification Report
Audit Boards
Suggest another round.
Final summary of all rounds and Audit Certification
RLA Tool
YES
Section 1-10.5-107(2),C.R.S
Last day for interested parties to request a recount of the Primary Election at their own expense.
Public

T+24 if Primary Election
T+34 if General/
Coordinated Election

Secretary of State

Audit Boards

RLA Tool

Public

Rule 25.2.4

Last day for county that conducted a comparison risk-limiting audit to review its CVR file and redact CVRs corresponding to any ballot card susceptible of being personally identified with an individual voter.

End

Exhibit B

SECURITY STANDARDS AND PROTOCOLS

I. State of Colorado Cyber Security Requirements
   a. System must meet security requirements posted by the State Chief Information Security officer. http://www.oit.state.co.us/ois/policies

II. Overall Systems Security
   a. If transmitting data over the internet or internally utilizing Transport Security Layer (TLS) the system must be capable of, at a minimum, utilizing TLS 1.2 and above. TLS is a cryptographic protocol that provide communications security over a computer network. The system must be configurable to support transmission encryption using TLS 1.0, TLS 1.1, and TLS 1.2 and at the Colorado Department of State's discretion, enforce TLS 1.2 and above. SSL connections are not permitted.
   b. The system must not store Personally Identifiable Information (PII) or sensitive information unless specifically authorized in writing by the Colorado Department of State. PII is information generally not publicly available that can be used to identify specific individuals. PII generally includes but is not limited to full dates of birth, driver's license numbers, state identification numbers, full or partial social security numbers, health insurance identifiers, etc. Approval must be specifically documented and approved for each data type that is considered PII.
   c. System must be hosted in a secure and industry-standard accredited facility, using dedicated hardware for the State of Colorado. Contractor will adhere to the National Institute of Standards and Technology's (NIST) guidelines for encryption, threat modeling, physical server security and tamper-detection monitoring.
   d. All Contractor systems will be protected by enterprise-grade firewalls and intrusion detection systems which enforce strict rules associated with each server within the data center.
   e. All servers must run operating system versions released within the past 4 years and must be fully supported by applicable vendors. All available security patches must be applied to operating systems unless a documented exception is approved by CDOS.
   f. Software packages installed on servers must be updated and maintained with the latest available, secure, and stable version. Any software that is not running the latest secure version must be submitted to CDOS for a possible documented exception.
   g. Application systems must have continuous self-monitoring functionality that proactively monitors the health of the application system. All files are inspected and scanned by an integrity monitoring system to ensure that no un-authorized modifications have been made to any file.
   h. Security protocols including the use of network firewall and Intrusion Detection Systems (IDS) that monitor all activity connecting to system networks must be utilized.
   i. Contractor must utilize enterprise grade Host Intrusion Prevention Software (HIPS) on each system. The HIPS software must be callable of blocking attacks and updated regularly.
   j. Application-aware firewall systems that block and deter suspicious activity from reaching application systems are utilized. Features include:
      i. Deep Packet Inspection — each inbound web request is scanned for suspicious activity; if suspicious activity is detected, inbound traffic will be dropped.

ii. Host-Based Blocking — if security perimeter detects a single computer that exceeds the limits of authentication attempts, that host is proactively blocked.
iii. User-Based Blocking — if the system detects a single user attempting to log in multiple times, the login credentials will be blocked.

k. Data Security and Destruction Protocols are followed. Data includes, but is not limited to:
    i. Systems and network security audit logs must be retained by contractor for one year. All logs must be provided to CDOS if requested.

l. All copies of data are securely destroyed after system is retired form use, or in accordance with the relevant local, state or federal laws. Contractor must request timeline for destruction of data from Colorado Department of State upon termination of contract or system retirement.

III. User Management

a. Username and Password requirements
    i. Use username/password features for all users that are configurable with CDOS security requirements.
    ii. Meet specific password complexity requirements for any application requiring a login.
    iii. Password length support for a minimum of 8 to 15 characters depending on CDOS requirements.
    iv. Password must contain three of the following:
        1. Upper case letter
        2. Lower case letter
        3. Number
        4. Symbol
    v. Password requirements must be easily adjustable to support increased security in the future. Changes to minimum length and complexity requirements must be configurable.

IV. System Load and Testing

a. Contractor must ensure uptime during petition cycles.
b. System components, as applicable, must be fault tolerant with Active/Passive failover capabilities at a minimum. All passive failover systems must be able to support full load without performance degradation.
c. Contractor must ensure proper backups are performed to ensure data may be recovered if altered or deleted.

V. Malicious File Detection

a. System is configured to scan for malicious content in files.
b. System must detection malicious scripts and/or active content in files such as Microsoft Office or PDF documents.

VI. Monitoring & Centralized Logging

a. System sends application and system logs to a centralized syslog server.
b. At a minimum the following entries for all system components must be logged.
    i. User ID
    ii. Type of Event

iii. Data and Time
iv. Success for Failure indication
v. Origination of event
vi. Identity of affected data or system

c. Systems audit logging and reporting must include details surrounding system and configuration changes.
d. System supports and is configured for synchronization with Network Time Protocol (NTP) servers.

VII. Encryption

a. The system is configured to secure encryption of data in transit and at rest. The system, at a minimum, uses encryption standards currently documented and validated for use by an agency of the U.S. federal government.
b. Disk and file encryption is configured with at a minimum AES 256 bit encryption.

VIII. Systems and Network Hardening

a. Meets industry best practices for hardening and security to prevent unauthorized access to the system.
b. System have secure network design with separation between front-end web interface servers, application servers and backend database servers. Systems must be separated by the equivalent of a network unified threat management firewall.
c. Contractor must ensure all systems are hardened according to industry best practice standards including the Center for Internet Security Hardening standards and applicable software and system hardening standards as specified by the software and/or hardware vendor. Systems hardening documentation must be available for CDOS review.
d. All systems must have vendor-supplied defaults for system passwords and other security parameters changed according to best practices.
e. Any sensitive data stored on systems must be encrypted. Sensitive data includes PII.
f. All systems with the capability to support anti-malware software must have up-to-date anti-malware software installed. All Windows based systems must have real-time antimalware scanning enabled. All Linux based systems must perform a full anti-malware scan at least weekly.
g. All systems must have file and/or configuration integrity monitoring software enabled and monitored for changes.
h. Ensure systems are set to use NTP for time synchronization.

IX. Network Segmentation

a. Proper network segmentation must be in place as applicable to the application. Web Services, mid-tier application servers, and databases must be segmented into separate security enclaves with only necessary traffic for system functionality permitted.
    i. Network segmentation must be documented with up-to-date network diagrams made available to CDOS.
    ii. A systems component inventory must be kept up-to-date and available for CDOS inspection.
    iii. Ensure wireless networks are not permitted in any internal enclaves supporting this system.

X. Systems Administration

a. All non-console administrator access is encrypted with strong cryptography.
b. All systems administrator access, local or remote, must be made from secure client devices that have up-to-date malware prevention, properly configured host based firewall, up-to-date operating systems, and other security controls to prevent misuse.
c. All non-console administrator access must utilize multi-factor authentication.
    i. Multi-factor authentication is defined as two out of the three following requirements:
        1. Something you have (Examples: token code, grid card)
        2. Something you know (Example: passwords)
        3. Something you are (Example: biometrics)
d. Multifactor authentication must support all authentication entries on the same screen.
e. Systems must enforce password changes for all accounts every 90 days or sooner.
f. Limit repeated access attempts by locking out accounts after not more than six attempts.
g. Set the account lockout duration to 2 hours or until and administrator unlocks the account.
h. If a session has been idle for more than 15 minutes, require administrator to re-authenticate to re-activate the session.

XI. Systems Access and Security
a. Workstations
    i. Must only be permitted to connect to necessary sites and system to perform documented business related tasks.
    ii. All workstations must have Advanced Malware Detection, such as Crowdstrike, and standard malware detection updated with real-time scanning enabled.
    iii. All workstations must have host based integrity monitoring, host based intrusion prevention, host based firewalls with only documented business permitted traffic, and continuous monitoring.
b. Server(s)
    i. Server must not be permitted to connect to the Internet over any protocols unless specifically documented and permitted by CDOS.
    ii. All servers must have Advanced Malware Detection and standard malware detection updated with real-time scanning enabled.
    iii. All servers must have host based integrity monitoring, host based intrusion prevention, host based firewalls with only documented business permitted traffic, and continuous monitoring.

XII. Web Application Firewall
a. All public facing web services and web applications must be protected by the following:
b. Web Application Firewall (WAF)
c. WAF must support both negative and positive attack prevention. Vendor must describe how they have implemented both negative signature detection and positive security model configuration.
d. Web Application Penetration testing annually and every time there is a significant change to the system.

XIII. Penetration Testing and Vulnerability Scanning

a. All systems must undergo external and internal network penetration testing annually and every time there is a significant change to the system.
b. Contractor must provide all medium and high level vulnerability findings from external network penetration testing and web application penetration testing to the Colorado Department of State within one week of the finding.
c. All critical and high rated vulnerabilities, determined by the penetration testing, must be mitigated within 72 hours. CDOS must approve of mitigation plan provided by vendor if a full patch for the vulnerability is not applied.
d. Contractor must allow external network penetration scans and testing from the Department of Homeland Security, the Colorado Department of State, and Colorado Department of State vendors.

XIV. Code Review

a. Ensure all code has a documented security review, focusing on the Open Web Application Scanning Project (OWASP) top 10, before being released to production.
b. Ensure all developers are trained on secure coding practices including the OWASP top 10.

Exhibit D

RLA Core System Requirements

The concept behind risk-limiting audits (RLAs) is to provide confidence in election outcomes. In furtherance of this goal, code developed to support RLAs must be available for public inspection and reuse.

Artifacts for the current RLA system are located at https://github.com/FreeAndFair/ColoradoRLA.

Requirement: System should have strong user management capabilities, including identifying user roles and privileges, and should implement password management functionality

Specifics from Colorado Implementation:

The system was integrated into an existing Active Directory. This allowed easy enforcement of standard password requirements such as minimum password complexity, length, expiration, account lockout, and password recovery and reset. User account attribute requirements were also added to the existing AD, and a new user group was added to identify RLA users and application permissions.

Requirement: System must support multi-factor authentication for all user access

Specifics from Colorado Implementation:

The system was integrated with an existing multi-factor system (Entrust). Colorado implements a two-factor access model using token codes or grid cards.

Requirement: System must meet CDOS system security requirements. Regular vulnerability scans will be required, penetration tests will be conducted, and access to all security monitoring and reporting artifacts of the system is required. As an entity of the State of Colorado, the system must meet security requirements posted by the Chief Information Security officer (http://www.oit.state.co.us/ois/policies).

Even though no personally identifiable information (PII) or federal tax information (FTI) is collected or maintained by the system, the security of post-election audit information is critical. PII is information generally not publicly available that can be used to identify specific individuals. PII generally includes but is not limited to full dates of birth, driver's license numbers, state identification numbers, full or partial social security numbers, health insurance identifiers, etc. FTI is taxpayer identification numbers specifically, and any information obtained by the Internal Revenue Service from tax returns.

Requirement: Personnel developing the system must be trained in and demonstrate secure coding practices.

Any system will be subject to web application penetration testing and static code analysis review. Developers must be trained on secure coding practices. Code must have a documented security review focused on the OWASP (Open Web Application Scanning Project) Top 10 before being released to production. Static code analysis and peer secure code review reports should be provided for every release.

Requirement: System must collect and retain system and application logs.

To allow investigation of issues and events, system and application logs must collect (at a minimum): user ID; type of event; date and time; success or failure indication; origination of event; and, identity of affected data or system.

Requirement: Code must be publicly available and developed under a GPL 3.0 license. GPL 3.0is a GNU General Public License 3.0: A specific variation of an open source license (see https://www.gnu.org/licenses/gpl-3.0.en.html).

Requirement: System must support common web browsers on common platforms for all functionality.

Browsers and platforms in wide use include Windows 7, 8, & 10, MacOS, Google Chrome, Mozilla FireFox, Microsoft Internet Explorer 11 and above, Microsoft Edge, and Safari.

Requirement: System must be based on modern languages and platforms with at least a 2-tier infrastructure design.

Specifics from Colorado Implementation:

The current tool is written in Java, with the reporting functionality written in Python 2.7. The system ran on Red Hat Enterprise Linux 7. Colorado used 2 web / application servers (combined) in primary / standby configuration. This was not configured to be an active-active configuration, nor was it configured to automatically failover due to design by the vendor. The webserver was Apache 2.4. The database layer was 3 RHEL7 servers running a PostgreSQL (9.6.5) database in a replicated configuration. The client/browser side is written in Node.js and React.

The system was hosted within the CDOS environment. This allowed CDOS the ability to leverage existing security systems and processes such support for Geographic Internet Protocol (GeoIP) blocking, web application firewall protection, system vulnerability management, Homeland Security vulnerability scanning, and other CDOS cybersecurity infrastructure measures. Geo IP blocking is the ability to restrict access from or to specific Internet Protocol addresses [*computers*] by the geographic location of the computer.

Appendix A –Cover/Signature Sheet

Request For Proposal
#CDOS-Elections-RFP-2018-001 Risk-limiting Audit software system

INSTRUCTIONS:

Offeror to complete this Response Sheet, sign in BLUE INK, and submit Proposal.

Offeror F.E.I.N.:		Payment Terms: (Minimum of Net 45)	
Proposal Delivery Date:			
Authorized Signature: *Signature acknowledges acceptance of all terms and conditions of the solicitation*			
Typed/Printed Name and Title:			
Company Legal Name:			
Doing Business As:			
Address:			
City:	State:	Zip:	
Phone Number:	Fax Number:		
Contact for Clarifications:			
Title:			
Phone Number:	Fax Number:		
E-mail Address:			

IMPORTANT NOTE: The following must be on the outside of the sealed Proposal Envelope/Container:
Offeror Name, Solicitation Number, Closing Date, Closing Time

Note: Telegraphic or electronic Proposals (Fax, Western Union, Telex, e-mail, etc.) cannot be accepted. Offerors are urged to read the solicitation document thoroughly before submitting a Proposal.

Offeror to answer and acknowledge by its signature above:

- Do you certify that the environmental attributes claimed in your Proposal are accurate: _____Yes ____ No
- Are you aware that the award notice will be published on the CDOS website ____ Yes ____ No
- Proprietary Information is in my response and as segregated pages: _____Yes _____No
- Registered with the Colorado Secretary of State ____ Yes ____ No
- Offeror proposes using Subcontractors for this project: _____Yes _____No
- Offeror has reviewed all Modifications made to this RFP: _____ Yes _____ No

Colorado Revised Statutes Title 24, Article 109, Entitlement to Cost, in part states: "When a protest is sustained administratively or upon administrative or judicial review and the protesting Bidder or Offeror should have been awarded the contract under the solicitation but, due to defect in the solicitation, was not, the protestor shall be entitled to the reasonable costs incurred in connection with the solicitation, including Bid preparation costs. No other costs shall be permitted and reasonable costs shall not include attorney fees."