



Request for Proposals

Electronic Recording Delivery System (ERDS)

**California Electronic Recording Transaction Network
Authority (CERTNA)**

222 West Hospitality Lane

First Floor

San Bernardino, California 92415

RFP: No. PS 07-01

TABLE OF CONTENTS

I. INTRODUCTION.....	1
A. PURPOSE	1
B. MINIMUM PROPOSER REQUIREMENTS.....	1
C. MANDATORY PROPOSAL CONFERENCE.....	1
D. CORRESPONDENCE.....	1
E. QUESTIONS	2
F. PROPOSAL SUBMISSION DEADLINE	2
G. ADMONITION TO BIDDERS.....	2
H. CONTRACT AWARD	2
I. DISPUTES RELATING TO PROPOSAL PROCESS AND AWARD	2
II. PROPOSAL TIMELINE	3
A. RELEASE OF RFP	3
B. MANDATORY PROPOSAL CONFERENCE	3
C. DEADLINE FOR QUESTIONS.....	3
D. DEADLINE FOR RECEIPT OF RFP RESPONSE	3
E. SEND AWARD/DENIAL LETTERS TO PROPOSERS (TENTATIVE).....	3
F. DEADLINE FOR APPEALS	3
G. TENTATIVE DATE FOR AWARDING OF CONTRACT(S)	3
III. PROPOSAL CONDITIONS	3
A. CONTINGENCIES	3
B. ACCEPTANCE OR REJECTION OF PROPOSALS	4
C. MODIFICATIONS	4
D. PROPOSAL SUBMISSION	4
E. INCURRED COSTS	4
F. NEGOTIATIONS.....	4
G. LEVELS OF SERVICE.....	4
H. DISCLOSURE OF CRIMINAL AND CIVIL PROCEEDINGS.....	4
I. FINAL AUTHORITY	5
IV. REQUIREMENTS	5
A. PROJECT SUMMARY	5
B. SCOPE OF WORK	5
C. TIMELINE AND COST PROPOSAL REQUIREMENTS	6
1. <i>Project Timeline</i>	6
i. <i>The Vendor shall present a Project Timeline for the entire project along with key milestones and deliverables. San Bernardino County will serve as the test environment for all project activities.</i>	6
D. COST PROPOSAL	6
i. <i>Professional Fees - System Design, Development, and Implementation</i>	6
ii. <i>Training Costs</i>	6
iii. <i>Travel Costs</i>	6
V. CONTRACT REQUIREMENTS	7
A. GENERAL.....	7
1. <i>Representation of the Authority</i>	7

2.	<i>Contractor Primary Contact</i>	7
3.	<i>Change of Address</i>	7
4.	<i>Contract Assignability</i>	7
5.	<i>Subcontracting</i>	7
6.	<i>Contract Amendments</i>	7
7.	<i>Termination for Convenience</i>	7
8.	<i>Attorney Fees and Costs</i>	8
9.	<i>Conflict of Interest</i>	8
10.	<i>Venue</i>	8
11.	<i>Jury Trial Waiver</i>	8
12.	<i>Invoices</i>	8
13.	<i>Notification Regarding Performance</i>	8
14.	<i>Improper Consideration</i>	9
15.	<i>Inaccuracies or Misrepresentations</i>	9
16.	<i>Employment of Former Authority Officials</i>	9
17.	<i>Recycling</i>	10
18.	<i>Legality and Severability</i>	10
19.	<i>Taxes</i>	10
20.	<i>Ownership of Documents</i>	10
21.	<i>Release of Information</i>	10
B.	INDEMNIFICATION AND INSURANCE REQUIREMENTS.....	10
1.	<i>Indemnification</i>	10
2.	<i>Insurance Coverage</i>	10
3.	<i>Additional Named Insured</i>	11
4.	<i>Waiver of Subrogation Rights</i>	11
5.	<i>Policies Primary and Non-Contributory</i>	12
6.	<i>Proof of Coverage</i>	12
7.	<i>Insurance Review</i>	12
C.	RIGHT TO MONITOR AND AUDIT.....	12
1.	<i>Right to Monitor</i>	12
2.	<i>Availability of Records</i>	13
D.	CALIFORNIA PUBLIC RECORDS ACT.....	13
VI. CONTRACT COMPLIANCE/EQUAL OPPORTUNITY		14
VII. FORMER AUTHORITY OFFICIALS		14
VIII. PROPOSAL SUBMISSION		14
A.	GENERAL.....	14
B.	PROPOSAL PRESENTATION.....	15
C.	PROPOSAL FORMAT.....	15
1.	<i>Cover Page</i>	15
2.	<i>Table of Contents</i>	16
3.	<i>Executive Summary</i>	16
4.	<i>Project Scope</i>	16
5.	<i>Approach</i>	16
6.	<i>Project Planning and Management</i>	16
6.1	<i>Project Timelines and Associated Milestones and Deliverables:</i>	16
6.2	<i>Scope Management Approach:</i>	17
6.3	<i>Risk Management Approach:</i>	17
6.4	<i>Client Communication Approach:</i>	17

6.5	Testing Approach and Plan:	17
6.6	Quality Management Approach:	17
6.7	Training Approach:	17
6.8	Documentation:	18
6.9	Knowledge Transfer Approach:	18
6.10	Resource Plan:	18
7.	System Description:	18
8.	System Development:	18
8.1	Development Methodology:	18
8.2	Technology Framework:	18
8.3	Application Architecture:	19
8.4	Hardware and Infrastructure Requirements:	19
9.	Transition:	19
10.	Interfaces:	19
11.	Non-functional Requirements:	19
12.	Cost and Pricing:	20
13.	Warranty:	20
14.	Proposal Assumptions:	20
15.	Exceptions:	20
16.	Alternate Proposals:	21
17.	Vendor Information and Qualifications:	21
17.1	General Company Information:	21
17.2	Resumes of the Project Team and Key Company Management:	21
17.3	Experience:	21
17.4	Company Financial Statements/Annual Report:	21
17.5	Project References:	22
17.6	Subcontractor Information:	22
18.	Statement of Certification:	22
19.	Insurance:	22
IX.	PROPOSAL EVALUATION AND SELECTION:	22
A.	EVALUATION PROCESS:	22
B.	EVALUATION CRITERIA:	23
1.	Initial Review:	23
2.	Evaluation:	23
C.	CONTRACT AWARD:	24
D.	DISPUTES RELATING TO PROPOSAL PROCESS AND AWARD:	24
E.	FINAL APPROVAL:	24
	ATTACHMENT A – COVER SHEET:	25
	ATTACHMENT B – COST PROPOSAL SPREADSHEET:	26
	ATTACHMENT C – STATEMENT OF CERTIFICATION:	27
	ATTACHMENT D – EXCEPTIONS TO RFP:	28
	ATTACHMENT E – SYSTEM VISION:	29

I. INTRODUCTION

A. Purpose

The California e-Recording Transaction Network Authority, hereafter referred to as the "Authority", is seeking proposals to provide an Electronic Recording Delivery System that includes software design and development, system implementation, training and documentation, and transition activities required to ensure that the Authority can competently maintain and operate the delivered system.

B. Minimum Proposer Requirements

All Proposers **must**:

1. Have a representative at the mandatory proposal conference as referenced in this Request for Proposal (RFP).
2. Have no record of unsatisfactory performance. Proposers who are or have been seriously deficient in current or recent contract performance, in the absence of circumstances properly beyond the control of the Proposer, shall be presumed to be unable to meet this requirement.
3. Have the administrative and fiscal capability to provide and manage the proposed services and development effort.
4. Have at least 5 years experience providing this type of software implementation.
5. Customer References – All Proposers must provide a minimum of three (3) references, involving the Proposer's delivery of services that demonstrate the ability of the Proposer to execute a project of this size and with similar requirements.

C. Mandatory Proposal Conference

A mandatory proposal conference will be held at the Hall of Records, 222 West Hospitality Lane, San Bernardino, California, in the Conference Room on the fourth floor on **Thursday, November 15, 2007 at 10:00 a.m. (Pacific Time)**. Attendance at the conference is **mandatory**. **No proposal will be accepted from any Proposer who fails to attend the proposal conference.**

D. Correspondence

All correspondence, including proposal, is to be submitted to:

CERTNA
Hall of Records
ATTN: Patrick Honny (RFP # PS-0701)
222 W. Hospitality Lane, First Floor
San Bernardino, CA 92415

Email: Patrick.Honny@SBCounty.gov

E. Questions

Questions regarding the contents of this proposal must be submitted in writing and directed to the individual listed above. Any questions responded to by the Authority will be answered and disseminated to all qualified Proposers.

Questions regarding the RFP and/or process must be submitted on or before 5:00 p.m. (Pacific Time) on November 20, 2007.

F. Proposal Submission Deadline

All proposals must be received at the address listed in Section I, Paragraph D, no later than 2:00 p.m. (Pacific Time) on December 20, 2007. Facsimile or electronically transmitted proposals will not be accepted since they do not contain original signatures. Postmarks will not be accepted in lieu of actual receipt. Late or incomplete proposals will not be opened and, therefore, not considered.

G. Admonition to Bidders

As of the issuance of this RFP, Vendors are specifically directed not to contact Authority personnel for meetings, conferences or technical discussions related to this RFP. Failure to adhere to this policy may result in disqualification of the Vendor. All questions regarding this RFP can be presented in writing as indicated in Paragraph E.

H. Contract Award

Contract(s) will be awarded based on a competitive selection of proposals received. A recommendation will be made to the Authority Board of Directors. The Board makes the ultimate determination regarding award of contract. The contents of the proposal of the successful Vendor will become contractual obligations and failure to accept these obligations in a contractual contract may result in cancellation of the award. The Authority reserves the option to make award(s) as it deems to be in the best interest of the Authority. Cost of service is an important factor in the evaluation process, but the Authority is not obligated to accept the lowest cost proposal. Ability to provide a quality service in a timely manner at a low or reasonable cost in accordance with the RFP requirements is critical to a successful proposal.

I. Disputes Relating to Proposal Process and Award

Vendor may appeal the recommended award or denial of award, provided the following stipulations are met:

- Appeal must be in writing.
- Must be submitted within ten (10) calendar days of the date of the recommended award or denial of award letters.

An appeal of a **denial of award** can only be brought on the following grounds:

- Failure of the County to follow the selection procedures and adhere to requirements specified in the RFP or any addenda or amendments.

- There has been a violation of conflict of interest as provided by California Government Code Section 87100 et seq.
- A violation of State or Federal law.

Appeals will not be accepted for any other reasons than those stated above. All appeals must be sent to:

CERTNA
Hall of Records
ATTN: Patrick Honny (RFP # PS-0701)
222 W. Hospitality Lane, First Floor
San Bernardino, CA 92415

A written response will be sent within ten (10) calendar days of receipt of the appeal/protest, unless more time is required to investigate and prepare the response, advising of the decision with regard to the appeal/protest and the basis for the decision.

II. PROPOSAL TIMELINE

- | | |
|--|--|
| A. Release of RFP | October 25, 2007 |
| B. Mandatory Proposal Conference | November 15, 2007, 10:00 a.m.
<i>RSVP with number of attendees</i>
<i>to Patrick.Honny@SBCounty.gov</i>
<i>by November 12, 2007</i> |
| C. Deadline for Questions | November 20, 2007, 5:00 p.m. |
| D. Deadline for Receipt of RFP
Response | December 20, 2007, 2:00 p.m. |
| E. Send award/denial letters to
Proposers (tentative) | January, 2008 |
| F. Deadline for appeals | 10 Calendar days from award
date. |
| G. Tentative date for awarding of
Contract(s) | February, 2008 |

III. PROPOSAL CONDITIONS

A. Contingencies

This request for proposal (RFP) does not commit the Authority to award a Contract. The Authority reserves the right to accept or reject any or all proposals if the Authority determines it is in the best interest of the Authority to do so. The Authority will notify all Proposers, in writing, if the Authority rejects all proposals.

B. Acceptance or Rejection of Proposals

Proposals shall remain open, valid and subject to acceptance anytime within one hundred eighty (180) days after proposal opening and up to the end of the agreement period.

C. Modifications

The Authority reserves the right to issue addenda or amendments to this RFP.

D. Proposal Submission

To be considered, all proposals must be submitted in the manner set forth in this proposal. It is the Proposer's responsibility to ensure that its proposal arrives on or before the specified time. All proposals and materials submitted become the property of the Authority.

E. Incurred Costs

This RFP process does not commit the Authority to pay any costs incurred in the preparation of a proposal in response to this request, and Proposer agrees that all costs incurred in developing this proposal are the Proposer's responsibility.

F. Negotiations

The Authority may require the potential Contractor(s) selected to participate in negotiations, and to submit revisions to pricing, technical information, and/or other items from their proposals as may result from negotiations.

G. Levels of Service

For any Contract awarded as a result of the RFP, the Authority makes no assurances regarding the minimum or maximum number of contracts awarded from this solicitation and the Authority cannot guarantee a minimum number of hours of service.

H. Disclosure of Criminal and Civil Proceedings

The Authority reserves the right to request the information described herein from the Vendor selected for contract award. Failure to provide the information may result in disqualification from the selection process and no award of contract to the Vendor. The Authority also reserves the right to obtain the requested information by way of a background check performed by an investigation firm. The selected Vendor also may be requested to provide information to clarify initial responses. Negative information provided or discovered may result in disqualification from the selection process and no award of contract.

The selected Vendor may be asked to disclose whether the firm, or any of its partners, principals, members, associates or key employees (as that term is defined herein), within the last ten years, has been indicted on or had charges brought against it or them (if still pending) or convicted of any crime or offense arising directly or indirectly from the conduct of the firm's business, or whether the firm, or any of its partners, principals, members, associates or key employees, has within the last ten years, been indicted on or had charges

brought against it or them (if still pending) or convicted of any crime or offense involving financial misconduct or fraud. If the response is affirmative, the Vendor will be asked to describe any such indictments or charges (and the status thereof), convictions and the surrounding circumstances in detail.

In addition, the selected Vendor may be asked to disclose whether the firm, or any of its partners, principals, members, associates or key employees, within the last ten years, has been the subject of legal proceedings as defined herein arising directly from the provision of services by the firm or those individuals. "Legal proceedings" means any civil action filed in a court of competent jurisdiction, or any matters filed by an administrative regulatory body with jurisdiction over the firm or the individuals. If the response is affirmative, the Vendor will be asked to describe any such legal proceedings (and the status and conviction thereof) and the surrounding circumstances in detail.

For purposes of this provision "key employees" includes any individuals providing direct service to the Authority. "Key employees" do not include clerical personnel providing service at the firm's offices or locations.

I. Final Authority

The final authority to award Contracts rests solely with the Authority's Board of Directors.

IV. REQUIREMENTS

A. Project Summary

- In July 2007, the Counties of San Bernardino and Kern entered into a Joint Powers agreement that established the California Electronic Transaction Network Authority (CERTNA) for the purpose of serving as the unifying umbrella agency to coordinate the services required to jointly develop, implement, and support a standardized electronic recording delivery system capable of being used by any number of submitters and counties that meet certain technical requirements.

B. Scope of Work

The scope of this project is to design, construct, and implement an Electronic Recording Delivery System for the Authority. This system must be compliant with the California Attorney General Regulations and be certified as such to be considered delivered. Once delivered and accepted, transition and training is to be conducted to ensure that Authority personnel can manage the system. Attachment E is a high level overview of system functionality as envisioned by the Authority. This attachment is provided for reference only. The Attorney General Regulations and System Certification requirements are the authoritative reference for system requirements and can be found at <http://aq.ca.gov/erds1/>.

C. Timeline and Cost Proposal Requirements

1. Project Timeline

- i. The Vendor shall present a Project Timeline for the entire project along with key milestones and deliverables. San Bernardino County will serve as the test environment for all project activities.

D. Cost Proposal

1. Vendor is to provide the cost proposal for Part 1 – 3 below. General instructions are provided for each section. Vendor should provide a milestone payment plan based on the receipt and acceptance of measurable deliverables. Payment terms are net 30 based on the receipt of the invoice and acceptance of deliverables.

- i. Professional Fees - System Design, Development, and Implementation

1. Professional fees associated with the design, development, and implementation costs should be provided. Total pricing should be provided as a fixed bid. The bidder must specify any and all expenses and charges for which the bidder expects reimbursement from the Authority. Additional options for pricing structures should also be provided that minimize the Authority's financial risk, allow for a phased approach, and maximize project success. Implementing modules of major systems is desirable as part of the phased approach, so that benefits can be achieved earlier and risk can be reduced.

- ii. Training Costs

1. Make sure that in the discussion of training costs that any assumptions such as the Authority providing the training facilities, and others are discussed in the training portion of the proposal. These assumptions should also be specifically stated when discussing what resources the Authority will need to provide.

- iii. Travel Costs

1. List all costs associated with travel and explain.

V. CONTRACT REQUIREMENTS

A. General

1. Representation of the Authority

In the performance of the Contract, Contractor, its agents and employees, shall act in an independent capacity and not as officers, employees, or agents of the Authority.

2. Contractor Primary Contact

The Contractor will designate an individual to serve as the primary point of contact for the Contract. Contractor shall notify the Authority when the primary contact will be unavailable/out of the office for (1) or more workdays. Contractor or designee must respond to Authority inquiries within three (3) business days. Contractor will also designate a backup point of contact in the event the primary is not available.

3. Change of Address

Contractor shall notify the Authority in writing, of any change in mailing address and/or telephone number within ten (10) business days of the change.

4. Contract Assignability

Without the prior written consent of the Authority, the Contract is not assignable by Contractor either in whole or in part.

5. Subcontracting

Contractor agrees not to enter into any subcontracting agreements for work contemplated under the Contract without first obtaining written approval from the Authority. Any subcontractor shall be subject to the same provisions as Contractor. Contractor shall be fully responsible for the performance of any subcontractor.

6. Contract Amendments

Any alterations, variations, modifications, or waivers of provisions of the Contract shall be valid only when they have been reduced to writing, duly signed and attached to the original Contract and approved by the required persons and organization.

7. Termination for Convenience

The Authority for its convenience may terminate this Agreement in whole or in part upon thirty - (30) days written notice. If such termination is effected, an equitable adjustment in the price provided for in this Contract shall be made. Such adjustment shall provide for payment to the Contractor for services rendered and expenses incurred prior to the effective date of termination. Upon receipt of termination notice Contractor shall promptly discontinue services unless the notice directs otherwise. Contractor shall deliver promptly

to Authority and transfer title (if necessary) all completed work, and work in progress, including drafts, documents, plans, forms, data, products, graphics, computer programs and reports.

8. Attorney Fees and Costs

If any legal action is instituted to enforce any party's rights hereunder, each party shall bear its own costs and attorneys' fees, regardless of who is the prevailing party. This paragraph shall not apply to those costs and attorneys' fees directly arising from a third-party legal action against a party hereto and payable under Section B.1 INDEMNIFICATION.

9. Conflict of Interest

Contractor shall make all reasonable efforts to ensure that no Authority officer or employee, whose position in the Authority enables him/her to influence any award of this contract or any competing offer, shall have any direct or indirect financial interest resulting from the award of this contract or shall have any relationship to the Contractor or officer or employee of the Contractor.

10. Venue

The venue of any action or claim brought by any party to this Agreement will be the Central District Court of San Bernardino County. Each party hereby waives any law or rule of the court, which would allow them to request or demand a change of venue. If any action or claim concerning this Agreement is brought by any third-party, the parties hereto agree to use their best efforts to obtain a change of venue to the Central District Court of San Bernardino County.

11. Jury Trial Waiver

Contractor and Authority hereby waive their respective rights by jury for any cause of action, claim, counterclaim, or cross-complaint in any action, proceeding, and/or hearing brought by either Vendor against Authority or Authority against Vendor on any matter arising out of, or in any way connected with this agreement, the relationship of Vendor and Authority, or any claim of injury or damage, or the enforcement of any remedy under any law, statute, or regulation, emergency or otherwise, now or hereinafter in effect.

12. Invoices

Contractor will generate invoices based upon milestones established within the Agreement.

13. Notification Regarding Performance

In the event of a problem or potential problem that could impact the quality or quantity of work, or the level of performance under this Contract, notification will be made within one (1) working day, in writing and by telephone to the Authority.

14. Improper Consideration

Vendor shall not offer (either directly or through an intermediary) any improper consideration such as, but not limited to, cash, discounts, service, the provision of travel or entertainment, or any items of value to any officer, employee or agent of the Authority in an attempt to secure favorable treatment regarding this Agreement.

The Authority, by written notice, may immediately terminate any Agreement if it determines that any improper consideration as described in the preceding paragraph was offered to any officer, employee or agent of the Authority with respect to the proposal and award process. This prohibition shall apply to any amendment, extension or evaluation process once an Agreement has been awarded.

Vendor shall immediately report any attempt by an Authority officer, employee or agent to solicit (either directly or through an intermediary) improper consideration from Vendor. The report shall be made to the supervisor or manager charged with supervision of the employee or to the Authority Administrative Office. In the event of a termination under this provision, the Authority is entitled to pursue any available legal remedies.

15. Inaccuracies or Misrepresentations

If in the administration of an Agreement, the Authority determines that Vendor has made a material misstatement, misrepresentation, or omission that materially inaccurate information has been provided to the Authority during the RFP process; the Agreement may be immediately terminated.

In the event of a termination under this provision, the Authority is entitled to pursue any available legal remedies.

16. Employment of Former Authority Officials

Vendor agrees to provide or has already provided information on former Authority, County of San Bernardino, or County of Kern administrative officials (as defined below) who are employed by or represent Vendor. The information provided includes a list of former administrative officials who terminated employment within the last five years and who are now officers, principals, partners, associates or members of the business. The information also includes the employment with or representation of vendor. For purposes of this provision, "administrative official" is defined as a member of the Board of Directors or such officer's staff, Board of Supervisors or such officer's staff, Authority Director or member of such officer's staff, County Administrative Officer or member of such officer's staff, County department or group head, assistant department or group head, or any employee in the Exempt Group, Management Unit or Safety Management Unit.

17. Recycling

Contractor shall use recycled and recyclable products whenever practicable in fulfilling the terms of the Contract. Recycled printed products shall include a symbol identifying the recycled material.

18. Legality and Severability

The parties' actions under the Contract shall comply with all applicable laws, rules, regulations, court orders and governmental agency orders. If a provision of the Contract is terminated or held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall remain in full effect.

19. Taxes

Authority is exempt from Federal excise taxes and no payment shall be made for any personal property taxes levied on Vendor or on any taxes levied on employee wages. The Authority shall only pay for any State or local sales or use taxes on the services rendered or equipment and/or parts supplied to the Authority pursuant to the Contract.

20. Ownership of Documents

All documents, data, products, graphics, computer programs and reports prepared by the Vendor pursuant to this Agreement shall be considered property of the Authority upon payment for product/services. All such items shall be delivered to the Authority at the completion of work under this Agreement, subject to the requirements of Section V.A.7 (Termination for Convenience). Unless otherwise directed by the Authority, Vendor may retain copies of such items.

21. Release of Information

No news releases, advertisements, public announcements or photographs arising out of this Contract or Proposer's relationship with Authority may be made or used without prior written approval of the Authority.

B. Indemnification and Insurance Requirements

1. Indemnification

The Contractor agrees to indemnify, defend and hold harmless the Authority and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages and/or liability arising from Contractor's acts, errors or omissions of any person and for any costs or expenses incurred by the Authority on account of any claim thereof, except where such indemnification is prohibited by law.

2. Insurance Coverage

Without in any way affecting the indemnity herein provided and in addition thereto, the Contractor shall secure and maintain throughout the Contract the following types of insurance with limits as shown:

- a) Workers' Compensation - A program of Workers' Compensation insurance or a State-approved Self-Insurance Program in an amount and form to meet all applicable requirements of the Labor Code of the State of California, including Employer's Liability with \$250,000 limits, covering all persons providing services on behalf of the Contractor and all risks to such persons under this Contract.

If Contractor has no employees, it may certify or warrant to Authority that it does not currently have any employees or individuals who are defined as "employees" under the Labor Code and the requirement for Workers' Compensation coverage will be waived by the Authority's Risk Manager.

With respect to Contractors that are non-profit corporations organized under California or Federal law, volunteers for such entities are required to be covered by Workers' Compensation insurance. If the Authority's Risk Manager determines that there is no reasonably priced coverage for volunteers, evidence of participation in a volunteer insurance program may be substituted.

- b) Comprehensive General and Automobile Liability Insurance - This coverage to include contractual coverage and automobile liability coverage for owned, hired and non-owned vehicles. The policy shall have combined single limits for bodily injury and property damage of not less than one million dollars (\$1,000,000).
- c) Errors and Omission Liability Insurance - Combined single limits of \$1,000,000 for bodily injury and property damage and \$3,000,000 in the aggregate.
- d) Professional Liability Insurance - Professional liability insurance with limits of at least \$1,000,000 per claim or occurrence.

3. Additional Named Insured

All policies, except for the Workers' Compensation, Errors and Omissions, and Professional Liability policies shall contain additional endorsements naming the Authority and its officers, employees, agents and volunteers as additional named insured with respect to liabilities arising out of the performance of services hereunder.

4. Waiver of Subrogation Rights

Except for the Errors and Omissions Liability and Professional Liability, Contractor shall require the carriers of the above-required coverages to waive all rights of subrogation against the Authority, its officers, employees, agents, volunteers, Contractors, and subcontractor.

5. Policies Primary and Non-Contributory

All policies required above are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the Authority.

6. Proof of Coverage

The Contractor shall immediately furnish certificates of insurance to Authority Department administering the Contract evidencing the insurance coverage, including the endorsements above required, prior to the commencement of performance of services hereunder, which certificates shall provide that such insurance shall not be terminated or expire without thirty (30) days written notice to Department. Contractor shall maintain such insurance from the time Contractor commences performance of services hereunder until the completion of such services. Within sixty- (60) days of the commencement of this Contract, the Contractor shall furnish certified copies of the policies and all endorsements.

7. Insurance Review

The above insurance requirements are subject to periodic review by the Authority. The Authority's Risk Manager is authorized, but not required, to reduce or waive any of the above insurance requirements whenever the Risk Manager determines that any of the above insurance is not available, is unreasonably priced, or is not needed to protect the interests of the Authority. In addition, if the Risk Manager determines that heretofore, unreasonably priced or unavailable types of insurance coverage or coverage limits become reasonably priced or available, the Risk Manager is authorized but not required, to change the above insurance requirements, to require additional types of insurance coverage or higher coverage limits, provided that any such change is reasonable in light of past claims against the Authority, inflation, or any other item reasonably related to the Authority's risk.

Any such reduction or waiver for the entire term of the Contract and any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Contract. Contractor agrees to execute any such amendment within thirty- (30) days of receipt.

C. Right to Monitor and Audit

1. Right to Monitor

Authority or any subdivision or appointee, thereof, and the State of California or any subdivision or appointee thereof, including the Auditor General, shall have absolute right to review and audit all records, books, papers, documents, corporate minutes, and other pertinent items as requested, and shall have absolute right to monitor the performance of Contractor in the delivery of services provided under this Contract. Contractor shall give full cooperation in any auditing or monitoring conducted.

Contractor shall cooperate with the Authority in the implementation, monitoring and evaluation of this Contract and comply with any and all reporting requirements established by the Authority.

2. Availability of Records

All records pertaining to service delivery and all fiscal, statistical and management books and records shall be available for examination and audit by Authority, Federal and State representatives for a period of three years after final payment under the Contract or until all pending Authority, State and Federal audits are completed, whichever is later.

D. California Public Records Act

All information submitted in the proposal or in response to request for additional information is subject to disclosure under the provisions of the California Public Records Act, Government Code Section 6250. Responses may contain financial or other data, which constitutes a trade secret. To protect such data from disclosure, Proposer should specifically identify the pages that contain confidential information by properly marking the applicable pages and inserting the following notice on the front of its response:

NOTICE

The data on pages _____ of this Proposal response, identified by an asterisk (*) or marked along the margin with a vertical line, contains information that is a trade secret. We request that such data be used only for the evaluation of our response, but understand that disclosure will be limited to the extent that the Authority of San Bernardino determines is proper under federal, state, and local law.

The proprietary or confidential data shall be readily separable from the Response in order to facilitate eventual public inspection of the non-confidential portion of the Response.

The Authority assumes no responsibility for disclosure or use of unmarked data for any purpose. In the event disclosure of properly marked data is requested, the Proposer will be advised of the request and may expeditiously submit to the Authority a detailed statement indicating the reasons it has for believing that the information is exempt from disclosure under federal, state and local law. This statement will be used by the Authority in making its determination as to whether or not disclosure is proper under federal, state and local law. The Authority will exercise care in applying this confidentiality standard but will not be held liable for any damage or injury that may result from any disclosure that may occur.

If confidentiality cannot be maintained, the Proposer has the option of withdrawing the Response to the Proposal or advising the Authority of its understanding that this information will become public record.

VI. CONTRACT COMPLIANCE/EQUAL OPPORTUNITY

The Vendor agrees to comply with Executive Orders 11246, 11375, 11625, 12138, 12432, 12250, Title VII of the Civil Rights Act of 1964, the California Fair Employment Practice Act, Equal Employment Opportunity, San Bernardino Authority Emerging Small Business Enterprise program, and other applicable Federal, State, and Authority laws, regulations, and policies relating to equal employment and contracting opportunities, including laws and regulations hereafter enacted.

VII. FORMER AUTHORITY OFFICIALS

Failure to provide this information may result in the response to the request for proposal being deemed non-responsive.

VIII. PROPOSAL SUBMISSION

A. General

1. All interested and qualified Proposers are invited to submit a proposal for consideration.
2. Proposals must be submitted in the format described below. Proposals are to be prepared in such a way as to provide a straightforward, concise description of

capabilities to satisfy the requirements of this RFP. Expensive bindings, colored displays, promotional materials, etc., are neither necessary nor desired. Emphasis must be concentrated on conformance to the RFP instructions, responsiveness to the RFP requirements and on completeness and clarity of content.

3. Proposals must be complete in all respects as required in this section. A proposal may not be considered if it is conditional or incomplete.
4. Proposals must be received no later than the date and time at the designated location as specified in Section I., Paragraph F - Proposal Submission Deadline.
5. All proposals and materials submitted become the property of the Authority.

B. Proposal Presentation

1. One bound original and 5 unbound copies (total of six) of the written proposal are required. The original copy must be clearly marked "Master Copy". If one copy of the proposal is not clearly marked "Master Copy", the proposal may be rejected. However, the Authority may at its sole option select, immediately after proposal opening, one copy to be used as the Master Copy. If discrepancies are found between two or more copies of the proposal, the proposal may be rejected. However, if not rejected, the Master Copy will provide the basis for resolving such discrepancies.
2. The package containing the original and copies must be sealed and marked with the Proposer's name and "CONFIDENTIAL – Electronic Recording Delivery System, RFP No: PS-0701.
3. All proposals must be submitted on 8 1/2" by 11" recycled paper with double sided printing, unless specifically shown to be impracticable, with no less than 1/2" top, bottom, left, and right margins. Proposals must be typed or prepared with word processing equipment and double-spaced. Typeface must be no more than 12 points. Each page, including attachments and exhibits, must be clearly and consecutively numbered at the bottom center of the page.
4. The Authority has adopted a recycled product purchasing standards policy, which requires Proposers to use recycled paper for proposals and for any printed or photocopied material created as a result of a Contract with the Authority. The policy also requires Proposers to use both sides of paper sheets for reports submitted to the Authority whenever practical.

C. Proposal Format

Response to this Request for Proposal must be in the form of a proposal package, which must be submitted in the following sequence and format:

1. Cover Page

Attachment A is to be used as the cover page for the proposal. This form must be fully completed and signed by an authorized officer of the Vendor.

2. Table of Contents

A complete Table of Contents for the entire proposal with respective page numbers opposite each topic.

3. Executive Summary

Vendors shall provide an Executive Summary that includes an overview of the proposed System development and implementation process, a summary of the System's principle features, the programming language utilized for System development, the database management system, testing and other tools to be used, and hardware requirements.

4. Project Scope

Include your understanding of the scope of this project including deliverables.

5. Approach

The Vendor is to provide their approach for the overall project. This section should also include the Vendor's methodologies for design, development, and implementation of the system. In addition, the Vendor is required to determine the scope of each phase (what business functionality is to be included and the sequence for development), the incorporation of the phases into the overall project plan, and the key deliverables for each phase. A phased approach implementing modules of the major systems is something that should be considered.

Vendor shall describe their phased development plan for an ERDS and include addressing the following questions:

- Describe your implementation methodology and strategy.
- How many implementations has the methodology been used on?
- Describe the methods used to develop overall project strategy, systems design, tools and methods to build the system, deployment strategy, system operation.
- Outline the tasks within each phase that would need to be accomplished in a successful implementation.
- Explain the costs and benefits associated with each proposed implementation approach.

6. Project Planning and Management

Please provide detailed responses to the following:

6.1 Project Timelines and Associated Milestones and Deliverables:

Provide a chart that clearly shows the project timeline including project phases and major milestones. Key deliverables for each phase should also be included.

6.2 Scope Management Approach:

The Vendor must provide their plan to manage scope throughout the project.

6.3 Risk Management Approach:

The vendor shall provide their approach to the management of risk, such as may occur with the release of software versions and updates and how the event of risk will be communicated. The risks of meeting requirements, user satisfaction, budget, and schedule in a project of this magnitude is significant. How will this be addressed in the implementation approach?

6.4 Client Communication Approach:

The Vendor shall be required to deliver a communications plan. The plan will describe the Vendor's approach that will be taken, the frequency and the type of mechanism that will be employed.

6.5 Testing Approach and Plan:

The Vendor shall present their recommended plan for system testing. Included in the response shall be a description of the testing methodology to be employed on this project including:

- Identification of the test management tool that will be employed and a description of the functionality it provides
- Identification of the defect tracking system that will be employed and a description of the functionality it provides

6.6 Quality Management Approach:

The Vendor is to describe how they plan to meet the requirements of Quality Assurance. Include in your response a description of how you will provide quality assurance for the following processes:

- 1 - Project Management Process
- 2 - Application Development Process
- 3 - Configuration Management
- 4 - Application Testing
- 5 - Release Management Process

6.7 Training Approach:

Provide a training plan that meets the needs of the following groups. (Include course recommendations and associated timelines as they relate to project phases.)

- Project Team

- Departmental Users
- System Support Staff

Also indicate training facility requirements including required space, number of workstations, and all necessary equipment

6.8 Documentation:

The response must also contain a complete listing of the documentation that the Vendor will provide the Authority to permit the successful takeover of ongoing system maintenance and operations.

6.9 Knowledge Transfer Approach:

The Vendor shall describe their approach to the transfer of knowledge with the respect to the System prior to completion of the project.

6.10 Resource Plan:

A resource plan is required. The plan must incorporate proposed project resources from the Vendor and the Authority's staff. The plan is to include proposed lines of responsibility, authority, and communication between project staff (responder, Authority, subcontractors, and Authority management). It must clearly outline the level of participation the Vendor requires from Authority staff during each phase of the Project.

In addition to staff resources from the Authority, this plan should include resource requirements in the form of facilities, equipment, supplies, system availability, etc. If not specifically mentioned it will be considered the responsibility of the vendor.

7. System Description

Your proposal response must contain sufficient information to clearly demonstrate your understanding of the Authority's requirements as described in Section IV.D. Unless otherwise stated, the vendor agrees to meet all of the requirements described in Section IV.D.

8. System Development

8.1 Development Methodology:

Describe in detail the software development methodology to be applied to the project and its benefits. Include a discussion of the lifecycle phases of the approach, and where you have successfully applied the methodology on other projects.

8.2 Technology Framework:

Provide an overview of the proposed system architecture including the following:

- Infrastructure tools that would be required

8.3 Application Architecture:

Provide a comprehensive overview of the proposed application architecture including major system components, interfaces, database, and software layer architecture. Design model documentation produced by an industry standard tool shall also be included.

8.4 Hardware and Infrastructure Requirements:

Provide a comprehensive overview and diagram of all hardware and infrastructure requirements including the following:

- Presentation Layer
- Application Layer
- Data Layer
- Third Party Software

9. Transition

Vendor shall provide a detailed overview of their proposed recommended transition strategy for moving from test to operational status.

10. Interfaces

The Vendor shall provide a detailed overview of their proposed interface strategy for the new system in an attached narrative to include creation of XML specifications.

11. Non-functional Requirements

Vendor shall provide a response to each of the following non-functional requirements. Note: the numbering scheme for non-functional requirements matches the same numbering scheme from the Non-Functional Requirements Section D.4. Your response should follow this numbering format.

Requirement ID	Non-functional Requirements	Response
4.1	Availability Requirements	
4.2	Efficiency Requirements	
4.3	Flexibility/Adaptability	

Requirement ID	Non-functional Requirements	Response
4.4	Integrity	
4.5	Interoperability	
4.6	Reliability	
4.7	Robustness	
4.8	Usability	
4.9	Capacity	
4.10	Scalability	
4.11	Reusability	
4.12	Maintainability	

12. Cost and Pricing

A cost proposal spreadsheet (Excel) is provided in Attachment B. Vendors must complete the cost template in Attachment B to submit proposal costs. Be sure to show all costs associated with this project.

13. Warranty

All services and deliverables provided in connection with this RFP shall be warranted for 12 months to perform in accordance with this RFP and any subsequent written agreement between the Authority and the Vendor. Vendor agrees that the information contained in their response to the RFP is correct, complete and current.

14. Proposal Assumptions

The Vendor shall provide a detailed list of all the assumptions made during the preliminary design as well as recommended next steps and required actions that shall be confirmed or corrected by the Authority before the development of the detailed design.

15. Exceptions

Complete Exceptions to RFP form (Attachment D) in which Vendor lists any exceptions to or deviations from the requirements of the RFP. Vendor must fully and clearly state and explain the basis for the exception. If there are not exceptions, a statement to that effect must be made. If the exceptions taken are contrary to Authority policy, at the sole discretion of Authority, the proposal may be rejected. Vendor's failing to note exceptions in their proposals will waive their rights to assert these exceptions during negotiations. Failure to abide by this rule is cause for termination of

negotiations. Vendors are obligated to review and fully understand the General Agreement Terms as condition of proposing.

16. Alternate Proposals

Alternate proposals will be considered if they meet the requirements of this RFP and if clear benefits and advantages are available to the Authority.

17. Vendor Information and Qualifications

Responses to this RFP should be structured so that a firm's qualifications can be readily evaluated. The following vendor information and qualifications are to be provided:

- General Company Information
- Resumes of the Project team and Key Company Management
- Experience
- Company financial statements
- Three project references
- Subcontractor information

17.1 General Company Information

Provide a brief description of your company and why you are well suited for this project.

17.2 Resumes of the Project Team and Key Company Management

Provide resumes of the proposed Project Team and key company management that are relevant to this project. Resumes should include a summary of education, training, and experience. Resumes should also clearly explain how the Vendor's staff has the experience, skills and ability to manage a project of this size and scope at the Authority of San Bernardino.

17.3 Experience

Provide information showing how the vendor meets the minimum of 5 years of required experience in complex information systems of this type and development projects of \$5 million or more.

17.4 Company Financial Statements/Annual Report

Vendor must provide the Company's Annual Report for the last two years **OR** independently audited financial statements for the most recent completed fiscal year. If audited financial statements are not available,

please provide unaudited financial statements along with a certification from the owner(s) and the Company's accountant that the information accurately reflects the company's current financial status. If the business is a sole proprietorship, please provide Schedule C of the Internal Revenue Service forms as well as a certification from the owner and the accountant that the information accurately reflects the business' current financial status.

17.5 Project References

Provide references from three (3) accounts on which the Vendor has developed complex information systems of this type. For each reference, provide the following information:

- Account name, address, and phone number
- Account contact name, title, address, email address, and phone number
- Provide a brief description of the project including size, scope, application, technology used, vendor resources involved, etc.

17.6 Subcontractor Information

If a Proposer plans to subcontract any portion of the service delivery described in the RFP, include a written justification for subcontracting. Attach a statement from each subcontractor signed by a duly authorized officer, employee or agent of the organization/firm that includes the name and address of the organization/firm, type of work to be performed and percentage of the total work of the proposal. Statement must also include that the subcontractor will perform all work as indicated and will comply with all items as indicated in this proposal.

18. Statement of Certification

Please complete, sign and date Attachment C.

19. Insurance

Submit evidence of ability to insurance in the amounts and coverages stated in Section V, Paragraph B - Indemnification and Insurance Requirements.

IX. PROPOSAL EVALUATION AND SELECTION

A. Evaluation Process

All proposals will be subject to a standard review process developed by the Authority. A primary consideration shall be the effectiveness of the agency or organization in the delivery of comparable or related services based on demonstrated performance.

B. Evaluation Criteria

1. Initial Review

All proposals will be initially evaluated to determine if they meet the following minimum requirements:

- a) The proposal must be complete, in the required format and in compliance with all the requirements of this RFP.
- b) Prospective contractors must meet the requirements as stated in the Minimum Proposer Requirements as outlined in Section I, Paragraph B.

Failure to meet all of these requirements may result in a rejected proposal. No proposal shall be rejected, however, if it contains a minor irregularity, defect or variation if the irregularity, defect or variation is considered by the Authority to be immaterial or inconsequential. In such cases the Proposer will be notified of the deficiency in the proposal and given an opportunity to correct the irregularity, defect or variation. The Authority may elect to waive the deficiency and accept the proposal.

2. Evaluation

Proposals meeting the above requirements will be evaluated on the basis of the following criteria:

- Strength and Stability of the vendor
 - Vendor demonstrates the depth and strength needed
 - Staff has the experience to support engagements of this size
 - Financial strength
 - References (past performance)
 - Resumes of team members
 - Bonding/Insurance
- Completeness and credibility of proposal
 - Demonstrates a clear understanding of Authority requirements
 - Proposed solution is feasible and minimizes risk
 - Complete and of sufficient detail to gain a clear understanding of what is being proposed
- Cost
 - Complete information is provided
 - Competitive and realistic

Selection will be based on determination of which proposal will best meet the needs of the Authority and the requirements of this RFP.

C. Contract Award

Contract(s) will be awarded based on a competitive selection of proposals received. The contents of the proposal of the successful Proposer will become contractual obligations and failure to accept these obligations in a contractual agreement may result in cancellation of the award.

D. Disputes Relating to Proposal Process and Award

No appeals process. Authority decision is final.

E. Final Approval

Any Contract resulting from this RFP will be awarded by final approval of the Authority Board of Directors.

ATTACHMENT A- COVER SHEET

PROPOSAL FOR ELECTRONIC RECORDING DELIVERY SYSTEM

VENDOR'S NAME (*name of firm, entity or organization*):

FEDERAL EMPLOYER IDENTIFICATION NUMBER:

NAME AND TITLE OF VENDOR'S CONTACT PERSON:

MAILING ADDRESS:

Street Address: _____

City, State, Zip: _____

TELEPHONE NUMBER: _____

FAX NUMBER: _____

EMAIL ADDRESS: _____

VENDOR'S ORGANIZATIONAL STRUCTURE

Corporation Partnership Proprietorship Joint
Venture

Other (explain): _____

If Corporation, Date Incorporated: _____ State Incorporated: _____

States Registered in as foreign corporation:

VENDOR SERVICES OR BUSINESS ACTIVITIES OTHER THAN WHAT THIS RFP
REQUESTS:

VENDOR'S AUTHORIZED SIGNATURE:

The undersigned hereby certifies that this proposal is submitted in response to this solicitation.

SIGNED: _____

DATE: _____

ATTACHMENT B – COST PROPOSAL SPREADSHEET

(Complete your response in EXCEL)

Vendor Cost Proposal (\$)				
Professional Fees	Phase 1	Phase 2	Phase 3	Phase 4
1) System design, development, and implementation costs – No. of phases will vary depending on each Vendor's proposal response				
Subtotal				
Training				
2) Training Costs				
Subtotal				
Travel and Expenses				
3) Travel and Expenses				
Subtotal				
4) Total Costs				

ATTACHMENT C – STATEMENT OF CERTIFICATION

The following statements are incorporated as part of our proposal

	Statement	Agree (initial)	Agree with qualification (initial and attach explanation)
1.	The offer made in this proposal is firm and binding for 180 days from the date the proposal is opened and recorded.		
2.	All aspects of this proposal, including cost, have been determined independently and without consultation with any other prospective Vendor or competitor for the purpose of restricting competition.		
3.	All declarations in the proposal and attachments are true and this shall constitute a warranty, the falsity of which shall entitle the Authority to pursue any remedy by law.		
4.	All aspects of the RFP and the proposal submitted shall be binding if the proposal is selected and a contract awarded.		
5.	The Authority will be provided with any other information the Authority determines is necessary for an accurate determination of our ability to provide the equipment and provide the services being proposed.		
6.	If selected, we will comply with all applicable rules, laws, and regulations.		

SIGNED:	_____
PRINT NAME:	_____
TITLE:	_____
DATE:	_____

ATTACHMENT D – EXCEPTIONS TO RFP

CONTRACTOR NAME _____

ADDRESS _____

Telephone# () _____ Fax # () _____

- I have reviewed the RFP and General Agreement Terms in their entirety and have the following exceptions: (Please identify and list your exceptions by indicating RFP, the Section or Paragraph number, and Page number, as applicable. Be specific about your objections to content, language, or omissions. Add as many pages as required)

Name of Authorized Representative _____

Signature of Authorized Representative _____ Date _____

ATTACHMENT E – SYSTEM VISION

ERDS Business Requirements

The San Bernardino County Auditor/Controller-Recorder (from here on, SBC) is spearheading work for a consortium of counties to allow electronic recording of notarized county documents, such as deeds of trust. The solution is referred to as Electronic Recording Delivery System (ERDS), within the context of the California e-Recording Transaction Network (CeRTN). CeRTN represents a consortium of counties that will allow these counties to develop and share standards to allow any California county or vendor to utilize an interoperable system that will electronically route scanned documents (digitized) and certain digital documents from participating vendors to county examiners in any participating county, optionally returning recorded documents, again, electronically, to the original vendor.

Currently, SBC has a proprietary system in place that allows it to service a current volume of approximately 1 million documents per year (3000-4000 per day). The desire is to fold this load into ERDS, and, within a year, additionally add Kern and other client counties which would bring volume to approximately 2 million documents yearly (6000-8000 per day). The ultimate vision is that all counties in California would participate in CeRTN, making this form of electronic recording the de facto standard thereby lowering the barriers to adoption.

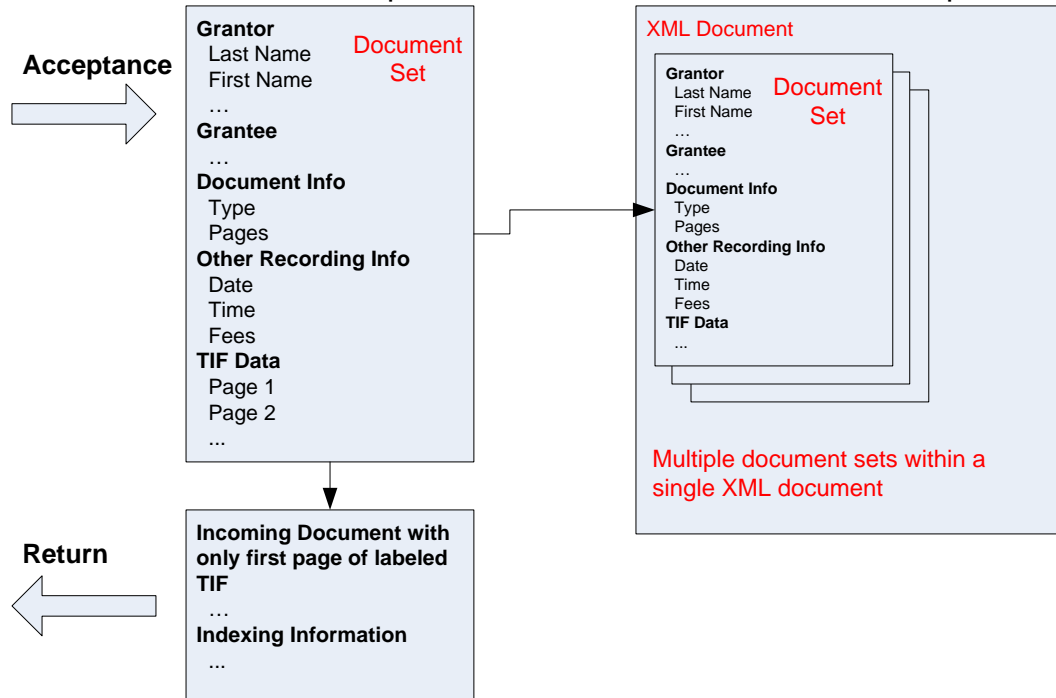
In essence, the main purpose of the ERDS solution is to perform the following tasks on behalf of authorized submitters and participating counties:

- Accept scanned documents (digitized) and certain digital documents to include recording information for individual customers from an authorized submitter via a secure web interface
- Accept scanned documents (digitized) and certain digital documents to include recording information for one or more customers packaged in an XML document via a secure web service
- Validate documents and track status throughout process
- Forward documents securely to appropriate counties
- Validate receipt of documents by respective counties
- Receive recorded documents after processing from respective counties
- Notify submitters of document status
- Provide recorded documents from counties to submitters

Throughout the acceptance and return cycles ERDS will monitor for fraud, maintain statistics, and keep a detailed audit trail of each action taken on a document or set of documents received.

The transmission of documents must be highly secure, as specified in the Technical Standards and Guidelines document submitted to the CeRTN Authority by SBC and the regulations as finalized by the California Department of Justice. The proposed solution must adhere to these standards in order to assure the confidentiality and integrity of documents that must be recorded in an electronic manner.

Note: The scope of the word “document” mentioned previously and from here on may be construed as an XML document whose payload consists of one or more complete sets of customer documents that must be recorded from the perspective of the authorized submitter. The pictorial below demonstrates this concept:



The return document will maintain the same format as the accepted document, but only the first page of TIF data in each document set will be returned as it is unnecessary to return the entire set of scanned TIF pages in the document set. Only the first page is required as it will have an electronic label stamped on the first page by the county examiner upon recordation.

Solution Proposal

The overall solution will consist of three main entities:

1. Authorized submitters (i.e., Title companies, banks, etc.)
2. CeRTN Hosted Environment (Tier IV Data Center) – the core of ERDS
3. Individual County Networks – will provide a specified component of ERDS at each site

Authorized submitters (from here on, “submitters”) will have the option to submit documents via a secure Submission/Tracking web application or web service. Typically, smaller Title companies would leverage the web application for individual customers, while larger entities, such as mortgage companies or banks, would submit

documents in bulk for multiple customers. All submitters will, however, have access to a Submission/Tracking web site to visually determine the status of submissions.

Document Submission

Documents from submitters using the web service option will be submitted in a defined XML format, which will include scanned TIF recording documents (digitized) or certain digital documents. CeRTN will be responsible for defining this standard and communicating the standard to submitters using the web service option. Submitters leveraging the web application will enter individual customer information and upload TIF documents to the web site. Once the user submitter uploads all relevant TIF documents, ERDS will package up these documents in XML for submission to the Payload Validation component of ERDS.

Document Validation and Status

The Session Manager server of the ERDS solution will consist of an internal application server that will parse and validate incoming documents. Validated documents will be stored in the ERDS SQL Server database. Invalid documents will not be stored, and the submitter will be notified of problems with the submitted documents. This should not be the case with documents submitted by the web application since the document packaging is controlled by ERDS, but this is expected for documents sent via the web service. XML documents submitted via the web service may have one or more document sets, and must be bound for the same county or they will be rejected. In both web application and web service cases, the final document transmitted to counties will be wrapped with control information relevant to processing by ERDS, which will be included in the document specifications.

Following are proposed document status values tracked by ERDS:

- Submitted

- Validated

- Invalid

- Transferred to County 'X'

- Received by County 'X'

- Received From County 'X'

- Accepted by County 'X'

- Rejected by County 'X' with appropriate reason codes

- Completed-Accepted (accepted and downloaded)

- Completed-Rejected (rejected and status checked)

Document Routing

After a document has been validated and stored, the document must then be routed to the respective county based on recording information in the document. This County

Connector server will reside in the ERDS DMZ, and will be notified by the Session Manager that there is a validated document that must be forwarded to its respective county. The County Connector will deliver the document to the Acceptance and Return server located in the DMZ of each respective county network, and update the document status accordingly. Note that CeRTN will support the county Acceptance and Return servers, and will provide specifications that each participating county must follow in order to integrate their backend systems to this server.

County Document Acceptance

When a document arrives at the county Acceptance and Return server, this document will be forwarded to the internal County Recorder System, and the Acceptance and Return server will notify the County Connector of receipt by the county. This connection will be developed and supported by the county. All recording tasks are now the responsibility of each county using existing systems, and the county is free to extract document sets out of the XML document as it sees fit to perform its processes. Once the county has approved or rejected a document, the county must prepare the document for return to the submitter. The return document must be packaged per specification and returned to the Acceptance and Return server, which will forward the document securely to the County Connector. This would include original control information packaged in the document upon acceptance.

County Document Processing

Once the County Connector receives a return document from the county Acceptance and Return server, it will contact the Session Manager for return validation of the document. The Session Manager will store the return document in the ERDS database, and then update the status of the document. Retention policies will determine when the original document is deleted after the return document has been received.

Document Return and Submitter Notification

Once the Session Manager has validated a return document, it may notify submitters via email, or simply allow submitters to access status information via the Submission/Tracking web site. At this point, submitters may download recorded documents from the web site or via the web service. Retention policies will be put in place to determine how long documents will be stored for access by submitters once they have successfully downloaded.

Note: Document return is optional for counties, as all counties may not have the appropriate technologies to participate in the document return process.

Document Specifications

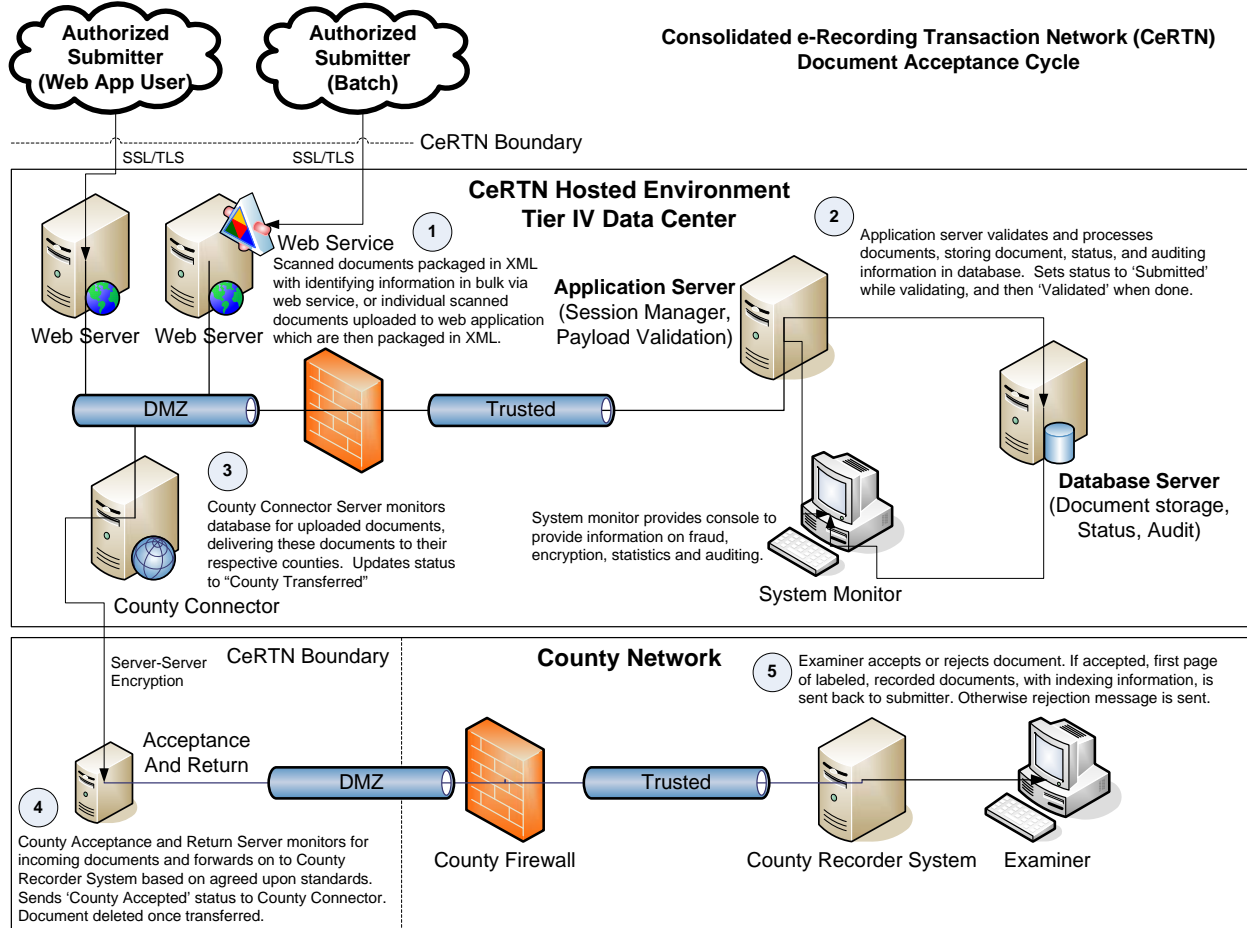
Document specifications must be developed for the following document types:

- Incoming submitter document – XML document that wraps document sets
- Parsed and validated document – Previous XML document with control information bound for counties
- Return documents – Schema for documents returned from counties including control information and recording data

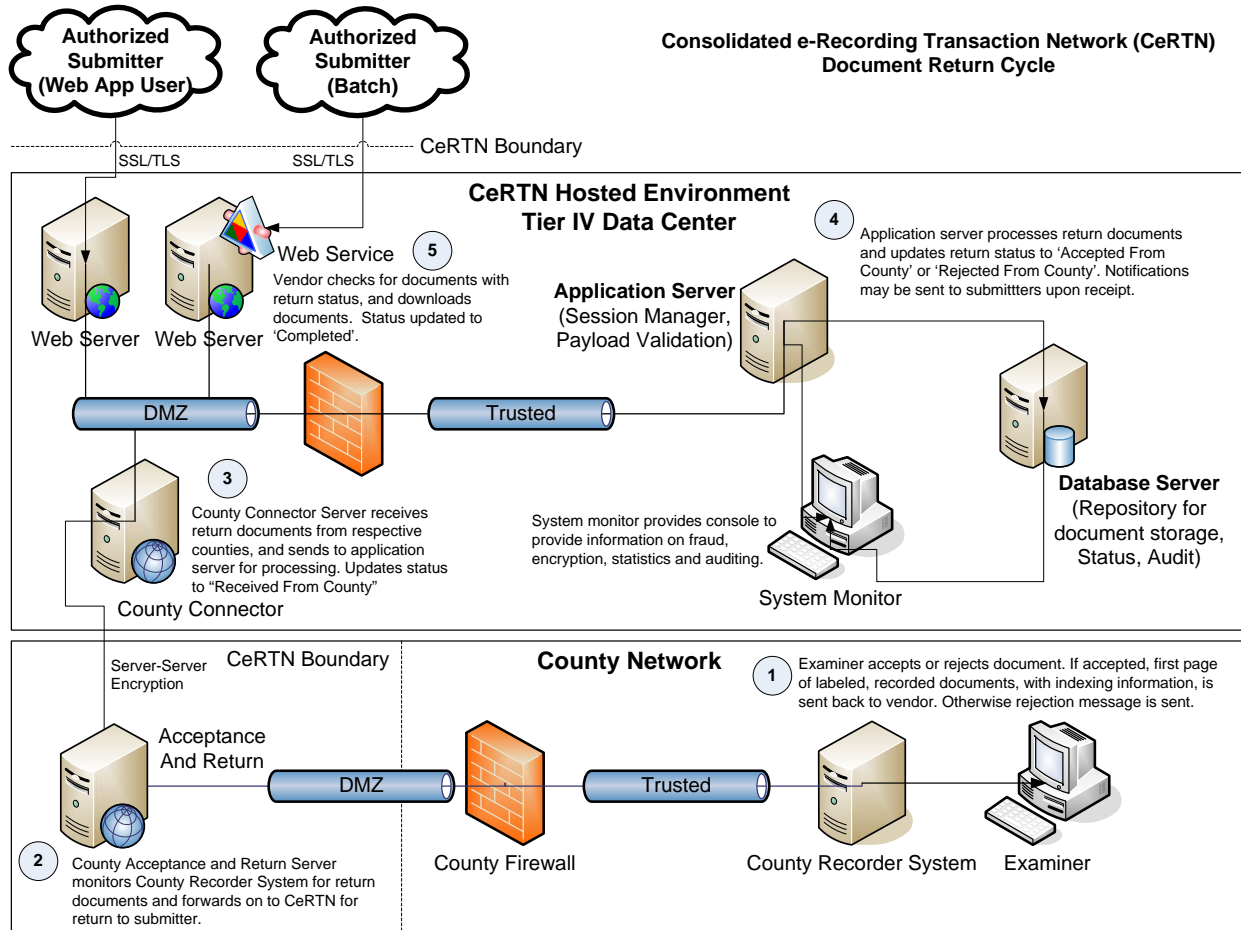
These specifications will be produced by CeRTN in cooperation with the participating counties.

Application Architecture

Below is a diagram of the proposed "Document Acceptance Cycle":



Next is a diagram of the proposed "Document Return Cycle":



The following key components (as mentioned in a previous section and specified in the diagrams above) are proposed for the ERDS application:

- Submission/Tracking Web Site
- Submission/Tracking Web Services
- Session Manager and Payload Validation Server
- System Monitor Application (Windows or Web)
- Database Server
- County Connector Server
- Acceptance and Return Server

Each component is outlined in more detail in the following sections.

Submission/Tracking Web Site

The Submission/Tracking web site is an ASP.NET 2.0 application running under IIS 6.0 on Windows Server 2003 or latest server OS, secured by SSL. It is a farm of web

servers residing in the DMZ of the CeRTN Hosted Environment. This web application will provide a browser-based user interface that will allow a user to enter the required customer information, and to upload title documents in TIF format that must be processed by the county. The site will also allow the user to determine status of uploaded documents as well as download of processed documents.

Submission/Tracking Web Services

The Submission/Tracking web services are also within the web farm in the DMZ of the CeRTN Hosted Environment. These web services will leverage WS-* standards and SSL to provide a secure environment for upload of one or more document sets as outlined in the requirements section above. Three web services will be provided to support submitters using the web service option:

- Document Submission
- Document Status
- Return Document

Upon document submission, the web service will return a control number to the submitter for each batch as well as validation status of submission. If this cannot be done in a reasonable period of time, then an option might be to return an incomplete validation status and allow the web service caller to call the status web service at a later time.

Provided with a control number, the Document Status web service will return status for each individual document set within an original XML document submission. The web service will also be able to return the status of any documents that do not have a 'Completed' status.

The Return Document web service will download each document set to a submitter along with control information that has an 'Accepted' status, or download relevant information on each document set that has a 'Rejected' status from the county.

Session Manager and Payload Validation Components

The Session Manager is a component on the Windows Server 2003 internal application server, within the CeRTN Hosted Environment, and is responsible for processing information from web application sessions and web service upload sessions. The Payload Validation components will also reside on this server.

Web Application Submissions (Individual)

For web application submissions, the Session Manager is responsible for managing the state of information and documents that are uploaded during a submission session. The Session Manager will package the information for delivery, assign control information, mark the status as 'Submitted', and then send to the Payload Validation component. If the payload is valid, the information is stored in the database by the Payload Validation component and the Session Manager will mark the status as 'Validated'. In this case, the payload should always be valid, as the web application shall validate all user input as well as verify that all uploaded documents are in the TIF format.

Web Service Submissions (Batch)

For web service submissions, the Session Manager will receive the XML document, wrap the document with control information, and mark its status to 'Submitted'. It will return a 'Submitted' status to the submitter, who may check ongoing status using the Document Status web service. It will then pass the document to the Payload Validation component for validation. The Session Manager will mark valid documents as 'Validated', and mark invalid documents as 'Invalid'.

System Monitor Application (Windows or Web Application)

The System Monitor application provides a console for the ERDS administrator to monitor for fraud and encryption violations, and to view statistics and audit trails. The Session Manager will be responsible for storing relevant information to the database as actions are performed.

Database Server

The SQL Server 2005 or latest shipping version database server will serve as the repository for all document storage, session status and auditing information. It will reside in a highly available cluster running 24x7x365. All programmatic access to the ERDS database will be coded with stored procedures.

County Connector Server

The County Connector is an application server running Windows Server 2003, residing in the DMZ of CeRTN. It resides in the DMZ because its responsibility is to be the point of contact for sending documents to participating counties as a part of the acceptance cycle, and receiving documents from participating counties as a part of the return cycle. This server may leverage either BizTalk Server or .NET 3.0 Windows Communication Foundation (WCF)/Windows Workflow Foundation (WF) components to perform all CeRTN to County communication and workflow functions. This will be a classic "buy versus build" decision during implementation planning.

The County Connector will be alerted by the Session Manager that there are documents ready for delivery to participating counties. The County Connector will then route documents to their respective counties via each county's Acceptance and Return server which will reside in each county DMZ. Upon successful transfer to a county, the County Connector will contact the Session Manager to update the status of a given document set to 'County Transferred'.

Acceptance and Return Server

The Acceptance and Return (from here on, A&R) server is an application server running Windows Server 2003, residing in the DMZ of each participating county. It will monitor for incoming documents routed by the County Connector in the CeRTN data center. Upon receipt, the A&R server will either forward documents to or allow pickup from the county recorder system, which is within the internal county network. Once the document has been transferred to the county internal network, the A&R server will notify the County Connector that the document status must be changed to 'Received by County'.

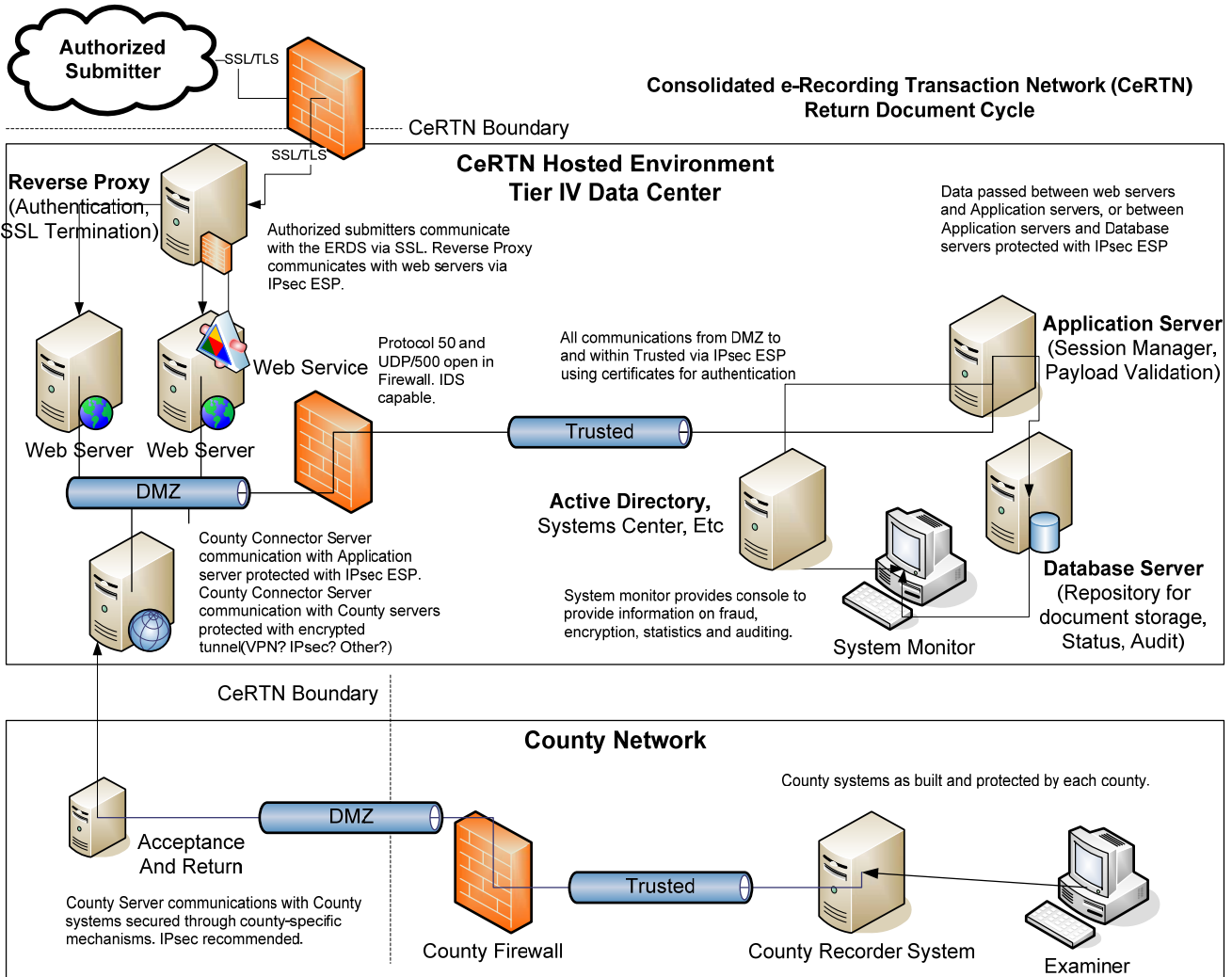
Return Process

As stated in the requirement section, return documents from participating counties is entirely optional, as some counties may not have the necessary infrastructure for return processing. For counties that are able to provide return documents, these recorded documents complete with recording information must be returned back to the A&R server for transmission to the County Connector. Only the first page of any scanned TIF documents in the payload will be returned, which will have the recording label required by the submitter.

When a return document is received by the A&R server, it will forward the document back to the County Connector. Once received by the County Connector, the document is stored in the ERDS database and the status is changed to 'Received From County'. The Session Manager will then process the return document and mark it as 'Accepted From County' or 'Rejected From County'. At this point, the Session Manager may notify submitters, or submitters may access ERDS via web site or web service to determine the status of their documents and perform downloads.

Network Architecture

Below is a diagram of the proposed "Network and Security Architecture":



The network and security architecture should meet or exceed the technical requirements.

Authentication Requirements:

1. Public Key Infrastructure (PKI). Security Level 2. FIPS 140-2, Security Requirements for Cryptographic Modules - May 25, 2001.
 - a. Provided by PKI Vendor (Thawte, GTE CyberTrust, etc.)
 - b. If the ERDS project determines to implement its own PKI, then the implementation will require an appropriate Hardware Security Module (HSM) on each Certificate Authority (CA) in order to meet FIPS 140-2 Level 2.
2. Private key issued to user for authentication and to verify the integrity and authenticity of ERDS payloads.
 - a. Web application (and any submitter-side web service) will use CAPICOM to use user's certificate to digitally sign the ERDS payload.
3. Type 1 and 2: Authentication consists of two-factors: User ID and password and PKI credentials on a token.

- a. Certificates issued to authorized submitters will be stored on a Smartcard in order to meet the NIST 800-63 Level 3 standards for two-factor authentication.
4. Third-party certificate authorities shall be on the list of certification authorities approved by the California Secretary of State.
 - a. Controlled by policy.
5. Each user shall be uniquely identified.
 - a. All users will have separate and unique accounts stored in Active Directory in the internal domain.
 - b. The certificates issued to authorized submitters will be mapped "one for one" to the accounts stored in Active Directory.
 - c. The provisioning process for authorized submitters must include:
 - i. The authorized submitter requests an appropriate certificate from the specific issuing CA.
 - ii. The authorized submitter supplies the certificate to the ERDS provisioning personnel.
 - iii. ERDS provisioning personnel create an Active Directory account for the authorized submitter, and associate the supplied certificate with that AD user account.
6. Shared user accounts and/or identity credentials are prohibited.
 - a. Controlled by administrative policy
7. User IDs shall either be based on the verified name of the user or a pseudonym approved by the County Recorder.
 - a. Controlled by identity provisioning process
8. User accounts shall be associated with ERDS roles to determine authorized actions.
 - a. Controlled by the ERDS application
9. Multi-County ERDS shall be capable of controlling access based on the county to which ERDS payloads are to be delivered and returned.
 - a. Controlled by the ERDS application
10. The standard for electronic authentication shall employ a token containing a cryptographic key such as a digital certificate and a password associated with a user ID. Authentication assurance shall meet level 3 per NIST Special Publication 800-63 - April, 2006.
 - a. The use of SmartCard-based certificates for authentication and for digital signatures of the ERDS payload meets this level of security.

Media Security Requirements

1. Payloads and encryption keys to be encrypted when stored on storage media with the same standards as when transmitting ERDS payloads.
 - a. All network communication paths carrying ERDS payloads are encrypted using IPsec/ESP
 - b. Database files are encrypted using Encrypting File System (EFS) built into Windows Server 2003.

Server Requirements

1. ERDS shall employ a proxy server for increased security.

- a. Internet Security and Acceleration (ISA) Server 2006 will be used as a reverse proxy.
2. ERDS server shall communicate via secure sessions through the proxy server when interoperating via the Internet.
 - a. All communications over the Internet are protected by TLS-based encryption with mutual authentication of server and workstation.
3. ERDS server shall run and control ERDS application software.
 - a. Controlled in the ERDS Application
4. ERDS server shall be configured to prevent unauthorized access, modifications, or use per:
 - a. NIST Security Configuration Checklists, SP 800-70 - May, 2005.
 - b. Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.
 - c. Microsoft's "Security Configuration Wizard" (SCW) will be the starting point for security settings for each server. This "wizard" incorporates the guidelines and settings found in the Windows Server 2003 checklist from NIST. As the NIST process proscribes, local operational requirements may drive some changes in the recommendations from the SCW.
5. Anti-malware software configured to start on system boot-up.
 - a. Anti-malware to be installed as part of the server build and configured to start automatically.
6. Host-based file integrity checking system configured to report on operating system file change.
 - a. Windows File Protection, built into Windows Server 2003, may suffice to meet this requirement. If not, other products, such as those from TripWire, may be evaluated to determine if they meet the full requirement.

Network Requirements

1. All ERDS transactions shall be protected with encryption.
 - a. All network communications are protected by IPsec/ESP.
2. Prior to a login sequence, a secure connection shall be established utilizing: TLS protocol with a minimum of 128-bit encryption; NIST Special Publication 800-63, Electronic Authentication Guideline - April, 2006; FIPS 197, Advanced Encryption Standard - November 26, 2001; Secure session shall be terminated when a user logs out or after a preset timeout limit of not more that 30 minutes, whichever occurs first.
 - a. All communications over the Internet are protected by TLS.
 - b. TLS will be configured to accept RSA with AES only.
 - c. The ISA Server will be configured to time-out sessions after 30 minutes.
 - d. The TLS session is the first part of meeting NIST 800-63 Level 3 requirements.
3. ERDS shall employ MAC to assure authenticity of encrypted ERDS payloads per FIPS 198, The Keyed-Hash Message Authentication Code (HMAC) - April 8, 2002.
 - a. The TLS specification requires HMAC.
 - b. As well, the digital signature of the ERDS payload will ensure integrity and authenticity of the payload.

4. Digital certificates shall be used to establish secure sessions between:
 - a. Users and the proxy server.
 1. All communications over the Internet are protected by TLS.
 - b. Proxy server and the ERDS server.
 1. All network communications are protected by IPSec/ESP.
5. ERDS components shall be protected from unauthorized network access via network perimeter security controls.
 - a. Employ stateful packet inspection.
 - b. Block unauthorized connections by limiting connection attempts addressed to ERDS components to those necessary for ERDS operation.
 - c. Configured to fail closed rather than open.
 - d. Detect possible intrusions and take action to prevent the intrusion and alert the ERDS administrator.
 1. *Consensus that the CeRTN design will incorporate a firewall with IDS capabilities.*
 2. *Perimeter will be protected by the appropriate Cisco firewall or equivalent.*

Workstation Requirements

1. Cisco's "Network Admission Control" (NAC) helps to ensure that client machines desiring "admission" to the network meet requirements set in a policy. Since all client machines are external to our ERDS network, NAC does not apply. No client machines will ever gain "admission" to the ERDS network, so there is no way to enforce policy compliance.
2. The ActiveX control used for the interactive submitter could contain code to scan the workstation and report back on any inconsistencies found. But this would not be considered a secure scan of the workstation. All it really might accomplish would be to help the "honest person remain honest." A malicious user would be able to subvert such a scan. The specific requirements for such a scan will have to be determined.
3. It will be difficult, if not impossible, to place technical controls to force the various workstation requirements. These requirements will likely have administrative controls followed by physical audit.

It is expected that the team shall be augmented, where appropriate, with customer resources that will have a stake in ultimate ownership of the solution at the end of the project. This will ensure appropriate knowledge transfer and effective adoption of the ERDS solution.

- **Program Manager** – Provides overall project oversight, resource and budget management
- **Project Manager/Business Analyst** – Provides daily project management, responsible for meeting business requirements

- **Architect (Application Development)** – Responsible for technical oversight and delivery of solution
- **Architect (Infrastructure)** – Responsible for oversight and selection of infrastructure environment
- **Developer Lead** – responsible for delivery of solution
- **Developer** – Responsible for delivery of solution
- **Test Lead** – Responsible for validation and verification that solution meets business requirements. Will also coordinate and drive user acceptance with ERDS resources.

The management team will work closely with ERDS business stakeholders and subject matter experts to further gather and refine requirements.

Hardware and Software Recommendations

Servers below may be logical or physical servers. If logical, then Windows Server 2003 R2 (Enterprise Edition) and Virtual Server 2005 R2 will be required on all physical servers that may accommodate the specifications below.

Server	Specifications	Software
Reverse Proxy Servers	2 Servers, 2 processors 4 GB RAM each	Windows Server 2003 R2 (Enterprise Edition), ISA Server 2006 (Standard Edition)
IIS Web Servers	4 Servers, 2 Processors, 2 GB RAM each	Windows Server 2003 R2 (Standard Edition)
Application Servers	2 Servers, 4 processors, 8 GB RAM each	Windows Server 2003 R2 (Standard Edition)
Database Servers	2 Servers, clustered, 4 processors, 8 GB RAM each	Windows Server 2003 R2 (Enterprise Edition)
Source Control Server	1 Server, 2 Processors, 2 GB RAM	Windows Server 2003 R2 (Standard Edition), Team Foundation Server
County Connector Servers	1 Server, 2 processors, 2 GB RAM	Windows Server 2003 R2 (Standard Edition)
County Return Server	1 Server per county, 2 processors, 2 GB RAM	Windows Server 2003 R2 (Standard Edition)
System Monitor workstation	1 workstation, 2 processors, 4 GB RAM	Windows Vista
Active Directory and Microsoft System Center	1 Server, 2 processors, 2 GB RAM	Windows Server 2003 R2 (Standard Edition), System Center 2007

Skill Sets to Support Solution

The skill sets to support this solution are similar to any Windows-based Internet application.

Provisioning and Identity Management – Use the tools to create and manage users of the system.

System Operations – Manage regularly occurring system tasks such as backup, monitoring, alert response, configuration management, update management, security update management, etc.

Database Operation – Maintain database and implement security measures to safeguard database.

Incident Management – Respond appropriately, following Incident Response Plan, to any anomalous occurrences in the system.

Helpdesk – Support users of the system as they encounter issues with the system.

System Load Capability

While it is impossible to predict the maximum load capability of the system before it is built, some general estimates may be made. We presume that the system will use some sort of transaction processing and message queuing to accept the document sets as they arrive. As long as the system can accept document sets from counties without loss of data, the actual processing of the document sets could take significantly longer.

At this point in the design, there is no way to estimate detailed system resources required for processing each document set. But with 8000 document sets of 300KB each, even modest systems would be able to manipulate in RAM, and write to disk the 2.4GB in a day. Complexity in the business rules and data manipulations will be an important factor, but these areas are best left to later phases of the project.

This use of queuing will essentially mean that network bandwidth is the limiting factor for the overall system. The table below shows some of the possible variations on accepting documents, making a few assumptions about document sizes.

Assumptions:

- One document set is 300KB
- One document set takes 600KB of network packets for IP overhead, IPSec, other inefficiencies.
- 8000 document sets will come in per working day.
- The working day is 8 hours long.

Network Speed	Document sets in 4 hours	Document sets in 8 hours	Document sets in 24 hours	Time for 8000 Doc sets
T1 (1.5 Mbps – 187.5K bytes/sec)	4500	9000	27K	~7 hours
Dedicated T3 (45 Mbps – 5625 Bytes/sec)	13.5K	27K	81K	~15 min

Even with a relatively slow network connection it should be possible to collect all document sets in each working day. If the number of daily document sets goes above about 9000, network speeds may need increasing beyond T1 capacity. As the system grows, or if performance is not acceptable, growing out the web layer while increasing the available network bandwidth should increase capacity to almost any level.

The system will have about 24 hours to process that day's document sets. (Although it could be less time available for processing. If the first of the document sets did not arrive until later in the morning, the system would still have to be complete with processing by start-of-day the next morning.) With 24 hours to process the 8000 document sets, the system has to be able to process about six document sets per minute. Since this amounts to less than 2 MB of data, it is not likely that even modest systems would have problems processing at this level. If six document sets per minute turns out to be difficult, growing out the application layer, and/or growing up the data layer should allow for significant increase in processing capability.