Electronic Recording Delivery System
System Certification Handbook

Addendum to the following ERDS Handbooks:
Baseline Requirements and Technology Standards
Vendor of ERDS Software Certification
Computer Security Auditor

Office of the Attorney General
California Department of Justice

November 2016

TABLE OF CONTENTS

SECTION 1 INTRODUCTION

The Electronic Recording Delivery Act of 2004 authorizes a County Recorder, upon approval by resolution of the Board of Supervisors and system certification by the ERDS Program, to establish an Electronic Recording Delivery System (ERDS) for the delivery, and, when applicable, return of specified digitized electronic records or digital electronic records that are an instrument of real estate transactions, subject to specified conditions, including system certification, regulation and oversight by the ERDS Program.

The Attorney General has established the ERDS Program within the Department of Justice, which is responsible for implementing the requirements of the law. In carrying out these duties this handbook describes procedures to obtain system certification and to establish the requirements and responsibilities of a County Recorder requesting certification of an ERDS. These procedures are supplement to the California Code of Regulations (CCR) Title 11, Division 1, Chapter 18, Articles 1 through 9 and the Baseline Requirements and Technology Standards Handbook.

A County Recorder requesting system certification to implement an ERDS for the delivery, and, when applicable, return of specified digitized electronic records and digital electronic records may obtain the Application for System Certification by downloading it from the ERDS web page at http://oag.ca.gov/erds.

Contact Information:

Department of Justice
Electronic Recording Delivery System Program
P.O. Box 160526
Sacramento, CA 95816-0526

Telephone: (916) 227-8907
Fax: (916) 227-0595

E-mail address: erds@doj.ca.gov
Web Page: http://oag.ca.gov/erds

SECTION 2 REQUIREMENTS AND RESPONSIBILITIES FOR ESTABLISHING AN ERDS

A County Recorder, either in his or her official capacity or by delegation of said responsibility, shall be responsible for administering an ERDS, ensuring that all ERDS requirements are met and shall oversee the assignment and delegation of said responsibilities by determining the necessary resources and means.

The County Recorder:

(A) Shall enter into a Memorandum of Understanding with the ERDS Program, before system certification, agreeing to the computed System Administration Fee and annually thereafter by an addendum to the Memorandum of Understanding;

(B) May implement an ERDS upon approval by the Board of Supervisors and system certification by the ERDS Program;

(C) Shall include in the ERDS a secure method for accepting for delivery, and, when applicable, return of digital electronic records or digitized electronic records that have been defined as an instrument within the California Code of Regulations (CCR), Title 11, Division 1, Chapter 18, Article 2 and the Baseline Requirements and Technology Standards Handbook;

(D) Shall be responsible for the overall safety and security of the ERDS;

(E) Shall be responsible for assigning specific ERDS privileges by contract or agreement to all Authorized Submitters whom shall ensure that an Agent, if any, complies with the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9;

(F) Shall enter into a contract with a Computer Security Auditor, with a valid Computer Security Auditor Certificate of Approval issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements of the CCR, Title 11, Division 1, Chapter 18, Article 9;

(G) Shall contract with a Vendor of ERDS Software, use in-house resources, and/or enter into an agreement with another public entity in implementing the ERDS. The County Recorder is required to verify prior to entering into a contract with a Vendor of ERDS Software, if any, that the Vendor has a valid Vendor of ERDS Software Certificate issued by the ERDS Program. This level of access requires fingerprinting for a state and federal criminal record check. (Refer to Section 4 of this handbook.); and

(H) Shall be the administrator of the ERDS, establishing and following ERDS Policies and Procedures that include the following:

(1) Define roles and responsibilities to ensure digital electronic records and digitized electronic records are correctly and securely submitted, delivered, and, when applicable, returned to the intended recipients. Textual or verbal disclaimers alone shall not be sufficient to control access to digital electronic records and digitized electronic records under the control of the ERDS;

(2) Maintain a list of all individuals designated as having secure and/or authorized access to operate the ERDS, and informing the ERDS Program of role changes by submission of the Change of ERDS Role (ERDS Form #0008). A copy of the list is to be maintained, for review during audits and local inspections;

(3) Ensure individuals with a secure access role understand and sign the Acknowledgement of Responsibilities (ERDS Form # 0012). A copy is to be maintained for review during audits and local inspections.

(I) Shall establish ERDS Operating Procedures and/or incorporate features within the ERDS design in order to restrict the instrument type and contents to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. (Refer to the Baseline Requirements and Technology Standards Handbook, section 1.3.5, ERDS Operating Procedures.)

SECTION 3 APPLICATION PROCESS

A County Recorder may apply for initial system certification of an ERDS designed as either a Single-County or Multi-County and designed as either a Type 1 or Type 2 or Type 1 and 2 operation, and, when applicable, return function via an ERDS. An ERDS shall not be operational prior to receipt of the ERDS Program's approval of the application and receipt of a System Certificate of Operation.

This section does not outline the addition of a County or Counties to an existing certified Single-County ERDS or to an existing certified Multi-County ERDS, which is a Substantive Modification detailed in Section 6 of this handbook.

(A) A Single-County ERDS application represents a single County's operation. A County Recorder, either in his or her official capacity or by delegation of said responsibility, initially applying for System Certification of a Single-County ERDS shall submit the following to the ERDS Program:

(1) A completed Application for System Certification (ERDS Form #0001A), which shall indicate the type of ERDS (e.g. Single-County and Type 1 or Type 2 or Type 1 and Type 2, and, when applicable, the return function), signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct; and

(2) All documentation as outlined in Section B of the Application for System Certification (ERDS Form #0001A). The documentation includes:

(a) A copy of the County Resolution, to implement the ERDS, as approved by the Board of Supervisors. The Resolution shall include, but not limited to; instrument type, Single-County, and, when applicable, the return function via an ERDS. For reference purposes, a sample Resolution is contained in the Appendices Section of this handbook. (It should be noted that each County's Resolution may be revised to meet its needs.);

(b) A copy of the Letter of Deposit, as proof that the ERDS source code materials have been placed in an approved escrow facility. Refer to Section 6.2 of the Baseline Requirements and Technology Standards Handbook for a description of the Letter of Deposit;

(c) A copy of the Vendor of ERDS Software contract, if any. If internal county resources or another public entity is being use to implement the ERDS, in lieu of a Vendor, it shall be stated in the County's Resolution;

(d) A copy of the County's contract with a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements to the ERDS;

(e) A copy of the successful Initial System Audit report, on the proposed ERDS, conducted by a Computer Security Auditor with a valid computer security auditor certificate issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements to the ERDS;

(f) Proof of fingerprint submission for individuals designated a secure access role and a copy of the list of all individuals with secure and/or authorized access. The fingerprint proof shall be met with fingerprint submission as outlined in Section 4 of this handbook; and

(g) A signed and dated Statement of Understanding (ERDS Form #0011) by the County Recorder, declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

The Statement of Understanding is an acknowledgement by the County Recorder that he or she understands the overall responsibility for administering the ERDS. This includes overseeing the assignment and delegation of said responsibilities and determining the necessary resources and means to accomplish the assignment.

(B) A Multi-County ERDS application represents where County Recorders collaborate and make use of a single ERDS serving multiple counties. In a Multi-County ERDS, one County Recorder will be designated as a "Lead County" Recorder and the collaborating County Recorder(s) will be designated as a "Sub-County" Recorder(s).

The Lead County Recorder, both in his or her official capacity or by delegation of said responsibility, shall be responsible for submission of the applications and has overall responsibility for administering the ERDS. The following outlines the submission requirements:

(1) Lead County Recorder

(a) A Lead County Recorder initially applying for a Multi-County system certification shall submit the following to the ERDS Program:

(1) A completed Application for System Certification (ERDS Form #0001A) which shall indicate the type of ERDS (e.g. Multi-County and Type 1 or Type 2 or Type 1 and Type 2, and, when applicable, the return function), signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct; and

(2) All documentation as outlined in Section B on the ERDS Application for System Certification (ERDS Form #0001A). The documentation includes:

(a) A copy of the Lead County's Resolution to implement a Multi-County ERDS as approved by the Board of Supervisors. The Resolution shall include, but not limited to, instrument type, Multi-County, and, when applicable, the return function via an ERDS. For reference purposes, a sample Resolution is contained in the Appendices Section of this handbook. (It should be noted that each County's Resolution may be revised to meet its needs.);

(b) A copy of the Letter of Deposit, as proof that the ERDS source code materials have been placed in an approved escrow facility. Refer to Section 6.2 of the Baseline Requirements and Technology Standards Handbook for a description of the Letter of Deposit;

(c) A copy of the Vendor of ERDS Software contract, if any. If internal county resources or another public entity is being use to implement the ERDS, in lieu of a Vendor, it shall be stated in the County's Resolution;

(d) A copy of the Lead County's contract with a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements to the ERDS;

(e) A copy of the successful Initial System Audit report, on the proposed ERDS, conducted by a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements to the ERDS;

(f) Proof of fingerprint submission for individuals designated a secure access role and a copy of the list of all individuals with secure and/or authorized access. The fingerprint proof shall be met with fingerprint submission as outlined in Section 4 of this handbook;

(g) All necessary documentation from the Sub-County(ies) shall be gathered and submitted as an attachment(s) to the Lead-County's application; and

(h) A signed and dated Statement of Understanding (ERDS Form #0011), by the County Recorder declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

The Statement of Understanding is an acknowledgement by the County Recorder that he or she understands the overall responsibility for administering the ERDS. This includes overseeing the assignment and delegation of said responsibilities and determining the necessary resources and means to accomplish the assignment.

(2) Sub-County Recorder(s)

A County Recorder applying as a Sub-County during the initial system certification of a Multi-County ERDS shall submit the following, to the Lead County Recorder for submission to the ERDS Program:

(a) A completed Application for Sub-County System Certification (ERDS Form #0001B), which shall be signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct; and

(b) All documentation as outlined in Section B on the Application for Sub-County System Certification (ERDS Form #0001B). The documentation includes:

(1) A copy of the Sub-County's Resolution to participate in a Multi-County ERDS as approved by the Board of Supervisors. Refer to the sample Resolution in the Appendices Section of this handbook. (It should be noted that each County's Resolution may be revised to meet its needs);

(2) Proof of fingerprint submission for individuals designated a secure access role and a copy of the list of all individuals with secure and/or authorized access. The fingerprint proof shall be met with fingerprint submission as outlined in Section 4 of this handbook; and

(3) A signed and dated Statement of Understanding (ERDS Form #0011), by the Sub-County Recorder declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

The Statement of Understanding is an acknowledgement by the Sub-County Recorder that he or she understands the overall responsibility for participating in a Multi-County ERDS. This includes overseeing the assignment and delegation of said responsibilities and determining the necessary resources and means to accomplish the assignment.

SECTION 4 FINGERPRINT PROCESS

All individuals in a secure access role, as defined in the CCR, Title 11, Division 1, Chapter 18, Article 4, section 999.121, shall submit fingerprint images to the Department of Justice for a state and federal criminal record check. All individuals designated a secure access role require fingerprint submission and clearance from the ERDS Program prior to serving in the role. (Refer to the CCR, Title 11, Division 1, Chapter 18, Article 4, section 999.122.)

The County Recorder, either in his or her official capacity or by delegation of said responsibility, or an Authorized Submitter may contact the ERDS Program for:

- The Request for Live Scan Service form (BCIA 8016ERDS) (Electronic Submission)
- Two FD 258 fingerprint cards (Manual Submission)

The following information will assist in fingerprint submission:

(A) Methods of Fingerprint Submission

(1) Live Scan Service (Electronic Submission)

All fingerprint submissions shall be transmitted electronically, via a Live Scan device, by a law enforcement agency and/or a certified public applicant agency providing such service.

To locate a Live Scan service site and information about their services, access the Attorney General website at http://oag.ca.gov or the Applicant Fingerprint Submission web page at http://oag.ca.gov/fingerprints.

(a) At the time of fingerprinting, the individual shall provide the Live Scan operator with the following:

(1) A completed Request for Live Scan Service form (BCIA 8016ERDS);

(2) The Live Scan fingerprint rolling fee. (Refer to Applicant Fingerprint Submission web page at http://oag.ca.gov/fingerprints); and

(3) The state and federal fingerprint processing fees. (Refer to the Fee Schedule in the Appendices Section of this handbook.)

(b) Upon completion of fingerprinting, the individual shall:

(1) Obtain the applicant copy and the contributing agency copy of the Request for Live Scan Service form (BCIA 8016ERDS) from the Live Scan operator, to be used as proof of fingerprint submission;

(2) Provide the County Recorder or Authorized Submitter with the contributing agency copy of the Request for the Live Scan Service form (BCIA 8016ERDS) as proof of fingerprint submission; and

(3) Retain the applicant copy of the Request for Live Scan Service form (BCIA 8016ERDS) as proof of fingerprint submission.

(2) FD 258 Fingerprint Card (Manual Submission)

If a Live Scan site is regionally unavailable, the DOJ has limited statutory authority to issue an exemption from electronic submission. If an exemption is sought, the individual shall use the FD 258 fingerprint card to have their fingerprints rolled by a law enforcement agency or certified public applicant agency. Contact the ERDS Program to obtain the FD 258.

To locate fingerprint service sites and information, access the Attorney General website at http://oag.ca.gov or the Applicant Fingerprint Submission web page at http://oag.ca.gov/fingerprints.

(a) At the time of fingerprinting, the individual shall provide the fingerprint roller with the following:

(1) Two completed FD 258 fingerprint cards; and

(2) The fingerprint rolling fee. (Refer to Applicant Fingerprint Submission web page at http://oag.ca.gov/fingerprints.)

(b) Upon completion of fingerprinting, the individual shall provide the County Recorder or Authorized Submitter with the following for submission to the ERDS Program:

(1) Two FD 258 fingerprint cards rolled by a law enforcement agency or certified public applicant agency fingerprint roller. The fingerprint cards shall include the fingerprint roller's signature and badge or certification number; and

(2) The state and federal fingerprint processing fees in the form of a check or money order made payable to the "California Department of Justice – ERDS Program". (Refer to the Fee Schedule in the Appendices Section of this handbook.)

(3) Residing Outside of California

Individuals residing outside of California that cannot have their fingerprints taken in California shall have their fingerprints rolled at a law enforcement agency in their state of residence.

(a) At the time of fingerprinting, the individual shall provide the fingerprint roller with the following:

(1) Two completed FD 258 fingerprint cards; and

(2) The fingerprint rolling fee. (Refer to your local law enforcement.)

(b) Upon completion of fingerprinting, the individual shall submit the following to the ERDS Program:

(1) Two FD 258 fingerprint cards rolled by a law enforcement agency in their state of residence. The fingerprint card shall include the fingerprint roller's signature;

(2) The state and federal fingerprint processing fees in the form of a check or money order made payable to the "California Department of Justice – ERDS Program". (Refer to the Fee Schedule in the Appendices Section of this handbook.)

(B) Fingerprint Status

Once the fingerprints are submitted, the DOJ processes the prints and notifies the ERDS Program with one of three responses: "No Record" (no criminal record); "Criminal Record" (criminal record present); or "Rejected" (poor quality fingerprints, missing or illegible data).

(1) "No Record" Response or Criminal Record Response with No Disqualifying Offense(s)

If the individual has no record or a record with no disqualifying offense(s), the individual, their employer, if any, the Computer Security Auditor and County Recorder shall be notified by the ERDS Program, in writing, that the individual is cleared to serve in a secure access role. The ERDS Program shall proceed with processing the application, if applicable.

(2) "Criminal Record" Response with Disqualifying Offense(s)

If the individual has a criminal record with a disqualifying offense(s), the individual, their employer, if any, the Computer Security Auditor and County Recorder shall be notified by the ERDS Program, in writing, that the individual is denied a secure access role. The ERDS Program shall proceed with processing the application, if applicable.

If the individual receives a denial, the individual can contact the DOJ to review and refute any erroneous or inaccurate information contained within their state criminal record and the Federal Bureau of Investigation for their federal criminal record. These reviews are outside of the ERDS Program.

An individual requesting to review their state record may contact:

California Department of Justice
California Justice Information Services Division
Bureau of Criminal Identification and Information
Record Information and Services Program
P.O. Box 903417
Sacramento, CA 94203-4170
(916) 227-3849

An individual requesting to review their federal record can obtain information at http://www.fbi.gov/howto.htm.

If it is determined through the record review process that an individual's record has been modified to reflect a record with no disqualifying offense(s), the individual may notify the County Recorder or Authorized Submitter. If a County Recorder wants to designate the individual in a secure access

role, the individual shall submit fingerprints for a state and federal criminal record check according to the submission methods outlined in this section. Once the fingerprints are submitted, the DOJ processes and notifies the ERDS Program with a state and federal criminal record result.

(3) Rejected Fingerprints

The fingerprint images shall be rejected, if the fingerprints are of poor quality, missing or illegible data, or the signature and certification number of the fingerprint roller are missing from the FD 258 fingerprint card. The ERDS Program shall notify the individual, in writing, of the rejection and provide resubmission instructions. The ERDS Program shall proceed with processing the ERDS application, if applicable.

(C) Subsequent Arrest and/or Disposition Notification

When an individual has been subsequently arrested and/or dispositioned, the DOJ shall notify the ERDS Program. The ERDS Program shall review the offense to determine if it disqualifies the individual from a secure access role.

If the individual has no disqualifying offense(s), the individual shall continue their secure access role and no notification will be sent.

If the individual has a criminal record with a disqualifying offense(s), the ERDS Program shall send a secure access termination letter, within ten business days, to the individual, their employer, if any, the Computer Security Auditor and County Recorder. The individual shall no longer serve in a secure access role.

To refute a disqualifying offense based on a subsequent arrest, the record review process can be pursued. If it is determined through the record review process, outlined in this section, that an individual's record has been modified to reflect a record with no disqualifying offense(s), the individual may notify the County Recorder or Authorized Submitter. If a County Recorder wants to designate the individual in a secure access role, the individual shall submit fingerprints for a state and federal criminal record check according to the submission methods outlined in this section.

(D) Re-fingerprinting of Individuals Changing Roles and/or Agencies

(1) When an individual who was previously cleared for a secure access role changes roles and/or agencies, changes employment or is designated additional secure access roles within the same agency; or if an employee or agent of an Authorized Submitter submits to one county and will now be submitting to multiple counties, re-fingerprinting is not required.

However, for such an individual the County Recorder shall submit a Change of ERDS Role (ERDS Form #ERDS 0008).

SECTION 5 APPLICATION REVIEW

The CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, established specifications, which are intended to assure that an ERDS is secure. The ERDS Program, through the application review process, shall review applications to determine if the requirements of the law are met. The ERDS Program shall provide, in writing, to the County Recorder, within an estimated timeframe of 90 days, an application review decision of approved, incomplete or denied.

(A) Approved

(1) If the application is approved, the ERDS Program shall send the following to the County Recorder:

(a) An approval letter; and

(b) A System Certificate of Operation, which authorizes the County Recorder to implement and operate the ERDS.

The System Certificate of Operation shall remain in effect, for the county or counties it was approved, without the need to renew, for the life of the ERDS unless there is a substantive modification, a suspension is issued or the County Recorder withdraws the ERDS certification.

(2) If the Request for Approval of Substantive Modification(s) (ERDS Form #0013) is approved, the ERDS Program shall send a letter to the County Recorder approving the removal of the provisional status, and the activation of the substantive modification from the ERDS production environment to the ERDS operational environment.

(B) Incomplete

(1) An application is incomplete when:

- The application has missing or illegible data;
- Supporting documentation, forms, applicable fees are not included with the application; and/or
- Proof of fingerprint submission was not submitted for individuals designated a secure access role.

(2) The ERDS Program shall return the incomplete application to the County Recorder with a written explanation and instructions on resubmission. It is the responsibility of the County Recorder to ensure that the application are corrected, completed and returned to the ERDS Program within 90 days.

The estimated ERDS Program's application review of 90 days is suspended until the resubmission is received by the ERDS Program.

In the case of a Multi-County ERDS, the applications shall be returned to the Lead County Recorder. It is the responsibility of the Lead County Recorder to ensure that the applications are corrected, completed and returned to the ERDS Program within 90 days.

If no response is received by the due date, the ERDS Program shall make one follow-up call to request the status of the resubmission. If the County Recorder is in the process of responding, a new due date shall be agreed upon by the ERDS Program and the County Recorder. The ERDS Program shall place a pending status on the resubmission. If no response is received by the new due date, the application shall be denied. The denial shall not prohibit the submission of an application at a later date.

(C) Denied

An application may be denied for good cause. Good cause shall exist when the individual does not satisfy the qualifications or system requirements, when it is necessary to protect the public interest, protect the integrity of public records or to protect homeowners from financial harm.

A denied letter, including the application, shall be sent to the County Recorder with an explanation for the denial. The denial shall not prohibit the submission of an application at a later date.

SECTION 6 PROCESS FOR SUBMITTING CHANGES TO AN EXISTING SYSTEM CERTIFICATION

(A) Non-Substantive Modification(s)

Following System Certification a non-substantive modification may occur. A non-substantive modification, as defined in the Baseline Requirements and Technology Standards Handbook, section 4.6, does not require a Modified System Audit; however, it shall be subject to review during audits and local inspections. Non-substantive modifications include, but are not limited to, the following:

(1) Addition and/or deletion of an individual(s) designated an ERDS role, by the County Recorder, who is authorized to use an ERDS for Type 2 instruments only. This ERDS role does not require fingerprinting.

No notification to the ERDS Program is required; however, a list of all individuals with secure and/or authorized access shall be maintained by the County Recorder, either in his or her official capacity or by delegation of said responsibility, and shall be subject to review during audits and local inspections.

(2) Addition and/or deletion of an individual(s) designated a secure access role as defined in the CCR, Title 11, Division 1, Chapter 18, Article 4, section 999.122.

(a) The County Recorder, either in his or her official capacity or by delegation of said responsibility, shall ensure the following requirements are met and shall be subject to review during audits and local inspections:

(1) A Change of ERDS Role (ERDS Form #0008) shall be submitted to the ERDS Program, with the added or deleted information for County Recorder employees and/or contract employees, Authorized Submitters or Agents, or the Vendor of ERDS Software employees and/or contract employees;

(2) An individual changing to a secure access role shall meet all fingerprint submission requirements. (Refer to Section 4 of this handbook.);

(3) Maintain a list of all individuals with secure and/or authorized access; and/or

(4) For secure access individual(s), an Acknowledgment of Responsibilities (ERDS Form #0012) shall be completed and signed by the individual, which is subject to review during audits and local inspections.

(3) Change of County Recorder

The new County Recorder, either in his or her official capacity or by delegation of said responsibility, shall notify the ERDS Program within 30 days. Submit a Statement of Understanding (ERDS Form #0011) signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(4) Change of Contact Information for a County Recorder

The County Recorder, either in his or her official capacity or by delegation of said responsibility, shall notify the ERDS Program in writing, within 30 days, by submitting the changed physical or mailing address, or other contact information.

(5) Withdrawal of Certification

(a) The County Recorder choosing to withdraw their ERDS certification, either in his or her official capacity or by delegation of said responsibility, shall notify the ERDS Program by submission of the following:

(1) An Application for Withdrawal (ERDS Form #0010) shall be completed, with a Cease of Operation/Service date, signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(2) A listing of all individuals authorized with secure and/or authorized access.

(3) A listing of all associated agencies and/or business entities authorized with secure and/or authorized access.

(b) In the case of a Multi-County ERDS, the Sub-County(ies) withdrawing shall complete and submit the Application for Withdrawal (ERDS Form #0010) to the Lead County Recorder. The Lead County Recorder shall be responsible for the submission to the ERDS Program.

Upon receipt of the Application for Withdrawal (ERDS Form #0010), the ERDS Program shall send a written acknowledgement to the County Recorder.

The withdrawal request shall render the System Certificate of Operation invalid. All ERDS operations, by law, shall cease as of the "Cease of Operation/Service Date" on the withdrawal application.

The withdrawal shall not prohibit the submission of an application at a later date.

(B) Substantive Modification(s)

Following initial system certification a Substantive Modification may occur. A Substantive Modification is defined as any change that affects the functionality of a certified ERDS. (Refer to Section 4.6 of the Baseline Requirements and Technology Standards Handbook.)

(1) Substantive Modification(s) shall require the following:

(a) The completion of a successful Modified System Audit report pertaining to only the components that are proposed to be modified and/or changed in the production environment. The report shall be completed by a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, and submitted to the County Recorder.

The modification and/or change shall remain on provisional bases, in the ERDS production environment, pending the application review and approval by the ERDS Program. Within 15 business days, of the provisional implementation, a copy of the successful Modification System Audit report shall be submitted to the ERDS Program as an attachment to the Request for Approval of Substantive Modification(s) (ERDS Form #0013) for application review. After ERDS Program approval, the provisional status shall be removed and the modification and/or change shall be activated in the ERDS operational environment.

(b) A Request for Approval of a Substantive Modification(s) shall be submitted, by the County Recorder, to the ERDS Program for application review as follows:

(1) The completed Request for Approval of Substantive Modification(s) (ERDS Form #0013), which shall be dated and signed declaring under penalty of perjury under the laws of California that all information is true and correct;

(2) A brief description of the functionality change to the ERDS shall be included in Section B; and

(3) All documentation as outlined in Section C. The documentation includes the following:

(a) Submit a copy of the revised County Resolution, as approved by the Board of Supervisors, to change the functionality of the ERDS;

(b) Submit a copy of the Letter of Deposit, as proof of ERDS source code materials being placed in an approval escrow facility;

(c) Submit a copy of the Vendor of ERDS Software contract, if any. If internal county resources and/or another public entity are being used to develop an ERDS in lieu of a Vendor, it shall be stated in the County Resolution;

(d) Submit a copy of the county's contract with a Computer Security Auditor, who has a valid computer security auditor certificate issued by the ERDS Program;

(e) Submit a copy of the successful Modified System Audit report completed by a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program;

If changing from a single-county to a multi-county ERDS:

(d) The Sub-County's completed Application for Sub-County System Certification (ERDS Form #0001B) signed and dated declaring under penalty of perjury under the laws of California that all information is true and correct and required documentation as follows:

(1) Submit a copy of the Sub-County's Resolution as approved by the Board of Supervisors;

(2) Submit proof of fingerprint submission for individuals designated a secure access role and a copy of the list of all individuals with secure and/or authorized access; and

(3) Submit a signed and dated Statement of Understanding (ERDS Form #0011), by the Sub-County Recorder, declaring under penalty of perjury the laws of California that all information is true and correct.

SECTION 7 AUDITS AND OVERSIGHT

The ERDS Program has responsibility for oversight and regulation of an ERDS. This responsibility shall be met by the Initial System Audit, Biennial Audits, Modified System Audits, Modified System Incident Audits and local inspections.

The audit schedule is:

Year 1 - Initial Security Audit
Year 2 - Local Inspection
Year 3 - Biennial Audit
Year 4 - Local Inspection
Year 5 - Biennial Audit

(A) The primary process for monitoring the effectiveness of security controls shall be computer security audits conducted by a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, for the purpose of conducting computer security audits and oversight requirements to the ERDS. These processes do not address prevention for any tampering or fraudulent documents prior to recording into an ERDS. A County Recorder shall contract with a Computer Security Auditor in order to meet all ERDS audit requirements. A list of Computer Security Auditors with a valid computer security auditor certificate is located on the ERDS web page at http:///oag.ca.gov/erds.

(B) A Computer Security Auditor shall conduct security audits of ERDS for the purpose of: 1) assessing the safety of the system; 2) verifying that the system is secure from vulnerabilities and unauthorized penetration; 3) ensuring ERDS operating procedures are in place and are being followed, and 4) validating that ERDS have no capability to modify, manipulate, insert, or delete information in the public record.

(C) The facility(ies) of a Type 2 only Authorized Submitter is exempt from a physical security audit and local inspection when the Computer Security Auditor has validated that all the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 have been met. In addition, including certification by the County Recorder and the ERDS Program that the method of submission allowed under the system will not permit an Authorized Submitter or its employees or agents, or any third party, to modify, manipulate, insert, or delete information in the public record or information in Type 1 documents, which are submitted for electronic recording.

Based on the Computer Security Auditor's findings, the ERDS Program reserves the right to conduct a physical audit of Type 2 only Authorized Submitter's facility(ies), if intrusion, fraud, or good cause has been found.

(D) Audits to meet the various ERDS requirements are as follows:

(1) Initial System Audit - To obtain initial system certification, a full system audit is required. "Initial" is defined as the "first time" System Certification application for either a Single-County or a Multi-County ERDS. This audit shall be performed prior to activating an ERDS for production and operation and shall be completed by a Computer Security Auditor. The Initial System Audit requirements and report format are detailed in Section 5 of the Baseline Requirements and Technology Standards Handbook.

A copy of the successful Initial System Audit report shall be submitted to the ERDS Program as an attachment to the Application for System Certification (ERDS Form #0001A). An ERDS shall not be operating prior to receipt of a System Certificate of Operations issued by the ERDS Program. A successful Initial System Audit shall be sufficient to meet the first year audit requirement.

(2) Biennial Audit – The Biennial Audit and local inspections of a lead county are required in alternating years to meet the ongoing oversight of a certified ERDS.

The Biennial Audit is a full system audit and shall be performed in the production and operational environments and shall be completed by a Computer Security Auditor and submitted to the County Recorder. A local inspection shall be performed in alternating years and shall be completed by the ERDS Program staff. The County Recorder shall submit a copy of the successful Biennial Audit report to the ERDS Program.

The Biennial Audit requirements and report format are detailed in Section 5 of the Baseline Requirements and Technology Standards Handbook; the local inspection requirements and report are detailed within this section.

(3) Modified System Audit – A successful Modified System Audit is required to obtain approval of a substantive modification(s) to a certified ERDS. The Modified System Audit shall pertain to only the components that are proposed to be modified and/or changed in the production environment. This report shall be completed by a Computer Security Auditor and submitted to the County Recorder. The modification and/or change to the ERDS shall remain on provisional bases, in the production environment, pending the application review and approval by the ERDS Program.

Within 15 business days, of the provisional implementation, a copy of the successful Modified System Audit report shall be submitted to the ERDS Program as an attachment to the Request for Approval of Substantive Modification(s) (ERDS Form #0013). After ERDS Program approval, the provisional status shall be removed and the modification and/or change shall be activated in the ERDS operational environment.

The Modified System Audit requirements and report format are detailed in Section 5 of the Baseline Requirements and Technology Standards Handbook.

(4) Modified System Incident Audit – A Modified System Incident Audit is required to meet the audit requirements resulting from an incident that compromises the safety or security of a certified ERDS. Incidents are detailed within Section 4.5 of the Baseline Requirements and Technology Standards Handbook, and details regarding incident reporting and ERDS operation are in Section 8 of this handbook.

A Modified System Incident Audit shall only pertain to the components that compromised the production environment and shall be performed prior to activating any correction in the ERDS production and operational environments. This Modified System Incident Audit shall be completed by a Computer Security Auditor, with a valid computer security auditor certificate issued by the ERDS Program, and submitted to the County Recorder. The County Recorder shall submit a copy of the successful Modified System Incident Audit report to the ERDS Program as an attachment to the detailed incident report. A successful Modified System Incident Audit shall not replace the Biennial Audit requirement. (References: the CCR, Title 11, Division 1, Chapter 18, Article 9; Baseline Requirements and Technology Standards Handbook; and Section 9 of this handbook.)

(E) Local Inspection

All lead counties associated with a certified ERDS shall be subject to a local inspection by an ERDS Program representative in alternating years of the Biennial Audit. Sub-Counties will be initially inspected and will then be subject to random scheduled inspection thereafter.

(1) Notification of Local Inspection

(a) An ERDS Program representative shall contact the County Recorder or his or her representative to schedule an on-site inspection of the ERDS and all associated processes.

(b) During a local inspection, the ERDS Program representative shall verify all of the following:

(1) That an auditable log is being maintained for two years;

(2) That all incident reporting documentation has been maintained and distributed as required;

(3) Access requests and inventory reports are maintained;

(4) The Computer Security Auditor reports are being maintained for a period of two years and the following are referenced: a list of all individuals with secure and/or authorized access; ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and contents to meet the requirements of the Electronic Recording Delivery Act of 2004 and the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9; safety and security of the system, including the vulnerability of an ERDS to fraud or penetration; results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies; recommendations for additional precautions needed to ensure that the system is secure; that reports and responses to recommendations are being sent to the Board of Supervisors, County Recorder, County District Attorney and the ERDS Program;

(5) For a Single-County ERDS, the ERDS Program representative shall verify a copy of the following is on file; System Certificate of Operation; County Resolution, County's ERDS Policies and Procedures, a signed Statement of Understanding (ERDS Form #0011), a list of all individuals with secure and/or authorized access, a signed Acknowledgement of Responsibilities (ERDS Form #0012) for all individuals with secure access, a completed Change of ERDS Role (ERDS Form #0008), Computer Security Auditor ERDS certificate and contract, Letter of Deposit, and Vendor of ERDS Software certificate and contract, if any.

(6) For a Multi-County ERDS, the ERDS Program representative shall verify a copy of the following is on file; System Certificate of Operation; County Resolution, County's ERDS Policies and Procedures, a signed Statement of Understanding (ERDS Form #0011), a list of all individuals with secure and/or authorized access, a signed Acknowledgement of Responsibilities (ERDS Form #0012) for all individuals with secure access, a completed Change of ERDS Role (ERDS Form #0008), Computer Security Auditor ERDS certificate and contract, Letter of Deposit, and Vendor of ERDS Software certificate and contract, if any.

In addition, on-site at the Lead County Recorders, for each county associated with the ERDS that a copy of the following is on file; Sub-County Resolution; Application for Sub-County System Certification (ERDS Form #0001B), a Statement of Understanding (ERDS Form #0011) signed by the Sub-County Recorder(s).

(2) Local Inspection Result

(a) The ERDS Program representative shall meet to discuss the Policy and Security Review report with the County Recorder or his or her representative. The report shall include the local inspection findings and a determination of compliant or noncompliant with ERDS security and operation requirements. The report shall be signed and dated by both the County Recorder or his or her representative and the ERDS Program representative. A copy of the report shall be provided to the County Recorder or his or her representative at the completion of the meeting. In the case of Multi-County ERDS, the lead County Recorder associated with the ERDS shall receive an informational copy.

(b) If the County Recorder is compliant, the ERDS Program shall send a compliant letter, within thirty business days of the inspection, to the County Recorder. In the case of Multi-County ERDS, the lead County Recorder associated with the ERDS shall receive an informational copy.

(c) If the County Recorder is non-compliant, the ERDS Program shall send a non-compliance letter, within thirty business days of the inspection, to the County Recorder. The letter shall include the non-compliant issue(s), the required action to be taken, and a due date allowing 30 days for correction and response. In the case of Multi-County ERDS, the lead County Recorder associated with the ERDS shall receive an informational copy.

(1) Upon receipt of the response, the ERDS Program shall complete an analysis determining whether the County Recorder has taken action and address the noncompliant issue(s).

If the response does satisfactorily address the noncompliance issue(s), the ERDS Program shall send a compliance letter to the County Recorder. In the case of Multi-County ERDS, the lead County Recorder associated with the ERDS shall receive an informational copy.

If the response does not satisfactorily address the noncompliance issue(s), the ERDS Program shall contact the County Recorder to work on resolving the noncompliance issues(s).

(2) If a response is not received by the response due date, the ERDS Program shall initiate a telephone call to the County Recorder to inquire on the status. If the ERDS Program and the County Recorder determine that an extension is needed, the response due date shall be extent by two weeks.

If no response by the extended response due date, the ERDS Program shall issue a suspension letter. (Refer to Section 9 of this handbook.)

(F) Report to the Legislature

Pursuant to Government Code section 27398(a), the Attorney General shall conduct an evaluation of all certified Electronic Recording Delivery Systems and report to both houses of the California State Legislature on or before June 30, 2009.

The evaluation shall be limited to the reporting of fraud occurrences and security breaches within the ERDS environments, as obtained through incident reporting, local inspections and audits.

(G) System Administration Fee

County Recorders shall pay for the direct cost of regulation and oversight by the ERDS Program. A System Administration Fee, as described in the Fee Schedule Appendices, in consultation with the interested County Recorders has been established to meet this requirement. A County Recorder shall enter into a Memorandum of Understanding with the ERDS Program, before system certification, agreeing to the computed System Administration Fee and annually thereafter by an addendum to the Memorandum of Understanding.

Failure to pay a County's proportionate share of the System Administration Fee, operating under a certified ERDS, shall result in the suspension of the System Certificate of Operation.

SECTION 8 INCIDENT REPORTING

Any incident of security violation(s) or suspected security violation(s) that compromise the safety or security of an ERDS, as outlined in the CCR, Title 11, Division 1, Chapter 18, Article 5, Section 999.146, shall be reported. The incident reporting process is as follows:

(A) County Recorder

The County Recorder, either in his or her official capacity or by delegation of said responsibility, shall establish criteria and procedures for handling and responding to incident(s), which shall be included in the county's ERDS Policies and Procedures.

In the case of a Multi-County ERDS, the Sub-County Recorders shall report incident(s) to the Lead County Recorder within two business days of the incident(s) date.

(1) The County Recorder, either in his or her official capacity or by delegation of said responsibility, shall completed and send a Fax Transmission Cover Sheet (ERDS Form #0007) to the ERDS Program.

(2) After the fax notification has been sent, the County Recorder, either in his or her official capacity or by delegation of said responsibility, shall complete a detailed incident report that shall include the following:

Date of the incident(s);
Parties involved (if known);
Nature and scope of the incident(s); and
Action(s) taken, including steps to protect against future incidents.

(3) The completed detailed incident report shall be sent to the ERDS Program, Computer Security Auditor, District Attorney, and Board of Supervisors within 10 business days of the incident(s) date. The County Recorder shall maintain the report for a period of two years and it shall be subject to review during audits and local inspections.

In the case of a Multi-County ERDS, the Lead County Recorder shall send an information copy to the Sub-County Recorder(s) associated with the ERDS. The Sub-County Recorder(s) shall be responsible for notifying their District Attorney(s), and Board of Supervisors.

A successful Modified System Incident Audit report shall be required, as outlined in Section 5 of the Baseline Requirements and Technology Standards Handbook and the CCR, Title 11, Division 1, Chapter 18, Article 9, and is submitted with the detailed incident report to the ERDS Program.

(4) Upon receipt of the detailed incident report, the ERDS Program shall:

(a) Send a written acknowledgement, within two business days to the reporting party;

(b) After an analysis is completed by the ERDS Program, an investigative result with the appropriate action to be taken, if any, shall be sent to the County Recorder, Computer Security Auditor that completed the successful Modify System Incident Audit report, Board of Supervisors, and District Attorney; and

In the case of a Multi-County ERDS, the Lead County Recorder shall send an informational copy to the Sub-County Recorder(s) associated with the ERDS. The Sub-County Recorder(s) shall be responsible for notifying their District Attorney(s), and Board of Supervisors.

(c) Maintain the reports for statistical purposes.

SECTION 9 SUSPENSION AND/OR TERMINATION OF CERTIFICATION

The ERDS Program, in close cooperation with County Recorders and public prosecutors, shall monitor the security of an ERDS. In cases of multiple fraudulent transactions, the ERDS Program shall order the suspension of an ERDS in any county or multiple counties for a period of up to seven days. If it is necessary to extend this order, the ERDS Program shall seek an order from the Superior Court. In addition, system certification may be withdrawn for good cause.

As used in this handbook, the terms "suspension" and "termination" are considered interchangeable and are used to designate removal of system certification of an ERDS.

(A) Suspension

The basis for suspension shall include, but is not limited to, the following:

(1) Unsatisfactory audit findings by the Computer Security Auditor on contractual agreement to perform computer security audits;

(2) Failure to respond to a corrective action, from the ERDS Program, for noncompliance issue(s) as a result of a local inspection;

(3) Failure to comply with the audit and local inspection schedule;

(4) Failure to annually enter into a Memorandum of Understanding with the ERDS Program for the System Administration Fee. (Refer to the Fee Schedule in the Appendices Section of this handbook.);

(5) Non-payment of a county's proportionate cost of the System Administration Fee. (Refer to the Fee Schedule in the Appendices Section of this handbook.);

(6) A reported security incident(s), that the ERDS Program has determined the ERDS is still vulnerable to intrusion;

(7) Non-compliance with the Statement of Understanding (ERDS Form #0011); and/or

(8) For good cause.

(B) Notification

The ERDS Program shall issue a letter of suspension, delivered by certified mail, notifying the County Recorder that the System Certificate of Operation is invalid and shall remain in valid until a reinstatement is granted through the reconsideration process. The County Recorder shall be instructed to immediately cease all ERDS operations as of the notification date. An informational copy shall be sent to the Board of Supervisors, Attorney General, and District Attorney.

In the case of Multi-County ERDS, all County Recorders associated with the ERDS shall receive an informational copy of the letter. The Sub-County Recorder(s) shall be responsible for notifying their District Attorney(s), and Board of Supervisors.

(C) Reconsideration

(1) A County Recorder may submit, to the ERDS Program, a reconsideration request, in writing, within 30 days of a suspension. The request shall include a justification for the reconsideration that addresses the reason(s) for suspension. Until the reconsideration decision is received from the ERDS Program all ERDS operations shall remain suspended.

(2) The ERDS Program shall complete an analysis and render a decision regarding the reinstatement. A letter shall be sent to the County Recorder with the ERDS Program's decision. An informational copy shall be sent to the Board of Supervisors, Attorney General, and District Attorney.

In the case of Multi-County ERDS, all County Recorders associated with the ERDS shall receive an informational copy of the letter. The Sub-County Recorder(s) shall be responsible for notifying their District Attorney(s), and Board of Supervisors.

SECTION 10 REQUEST FOR REPLACEMENT OF CERTIFICATE AND/OR DOCUMENT(S)

To ensure that an individual's right to privacy is enforced and that confidential information provided on documents submitted to the ERDS Program, is protected from threat of potential risk in the indiscriminate collection, maintenance and dissemination of information, the Request for Replacement of Certificate and/or Documents process was established. The process is as follows:

(A) To request copies of documents, complete and submit a Request for Replacement of Certificate and/or Documents (ERDS Form #0006), signed and dated declaring under penalty of perjury under the laws of the State of California that the requested documents pertain to his or her application submission to the ERDS Program. The appropriate fee shall accompany the request in the form of a check or money order made payable to "Department of Justice – ERDS Program". (Refer to the Fee Schedule in the Appendices Section of this handbook.)

(B) The fee shall be processed prior to completing the request.

SECTION 11 APPENDICES

A Sample Resolution
B Sample County's ERDS Policies and Procedures
C Fee Schedule
D Acronyms and Definitions

Appendix A SAMPLE RESOLUTION

[NOTE: EACH COUNTY'S RESOLUTION MAY BE REVISED TO MEET THEIR NEEDS.]

RESOLUTION OF THE COUNTY OF _____ BOARD OF SUPERVISORS APPROVING THE COUNTY OF _____ TO ESTABLISH AN ELECTRONIC RECORDING DELIVERY SYSTEM

WHEREAS, Assembly Bill 578, Chapter 621, September 21, 2004 added to the Government Code, Chapter 6, sections 27390 through 27399, and established the Electronic Recording Delivery Act (ERDA) of 2004. Government Code section 27391(a) authorizes a County Recorder upon approval by resolution of the Board of Supervisors to establish an electronic recording delivery system, for the delivery, and, when applicable, return of specified digitized electronic records and digital electronic records upon system certification by the ERDS Program.

WHEREAS, Government Code section 27397(c)(1) authorizes a County Recorder to impose a fee in an amount up to and including one dollar ($1) for each real property instrument that is recorded by county; and

WHEREAS, Government Code section 27397(c)(2) authorizes a County Recorder to impose a fee upon any Vendor seeking approval of software and other services as part of an electronic recording delivery system and upon any person seeking to contract as an Authorized Submitter; and

WHEREAS, the ERDS Program has established regulations and has been delegated the authority for system certification, regulations and oversight of Electronic Recording Delivery Systems and the County Recorder shall comply with all ERDS regulations; and

NOW, THEREFORE, BE IT RESOLVED that the County of _____ Board of Supervisors approves the County Recorder to:

- Establish a [i.e. Single-County ERDS or a Multi-County ERDS] for [i.e. Type 1 or Type 2 or Type 1 and Type 2 instruments], and, when applicable, the return function.

- Conduct all negotiations, execute and submit all documents necessary for the establishment of an Electronic Recording Delivery System.

- Impose a fee up to and including one dollar ($1) for each real property instrument that is recorded by the County.

- Impose a fee upon any person seeking to contract as an Authorized Submitter.

- Contract with [i.e. Vendor of ERDS Software, use in-house resources, and/or enter into an agreement with another public entity] in an ERDS implementation.

- Enter into a Memorandum of Understanding with the ERDS Program, before system certification, agreeing to the computer System Administration Fee and annually thereafter by an addendum to the Memorandum of Understanding.

- Issue payments to the ERDS Program for the County's proportionate share of the System Administrative Fee; and

NOW THEREFORE, BE IT FURTHER RESOLVED, that the County Recorder shall:

- Submit an application for system certification to the ERDS Program; and, in doing so will comply with the California Code of Regulations, Title 11, Division 1, Chapter 18, Articles 1 through 9; and

- Designate those individuals with secure and authorized access to an ERDS comply with Government Code section 27395(b); and

- Notify the ERDS Program if an individual that has secure access no longer requires that access comply with the California Penal Code section 11105.2(d); and

- Notify the Board of Supervisors, District Attorney, Computer Security Auditor on contractual agreement, and ERDS Program if there are any known or suspected security violations that compromises the safety and/or security of the ERDS; and

- Notify the ERDS Program if there is a change of County Recorder; and

- Notify the ERDS Program if the County wishes to withdraw their system certification.

THE FOREGOING RESOLUTION WAS DULY ADOPTED by the Board of Supervisors of the County of _____, State of California, on the_____.
(Day/Month/Year)

APPROVED BY:

_____
Signature of Board of Supervisor, Officer

_____
Signature of County Recorder, or Representative

Appendix B SAMPLE County's ERDS POLICIES and PROCEDURES

[A county's policies and procedures may be revised to meet its needs.]

ERDS POLICIES AND PROCEDURES

This sample has been developed to meet the security requirements and responsibilities for establishing an ERDS. The security of the ERDS shall be implemented through a combination of administrative, physical and technical controls.

A County Recorder or his or her representative shall be responsible for administering the ERDS, ensuring that all ERDS requirements are met and shall oversee the assignment and delegation of said responsibilities by determining the necessary resources and means. A County Recorder or his or her representative shall ensure the following:

1) That ERDS Operating Procedures are complete and in place assure the continuing security and lawful operation of the ERDS;

2) That the "Certified ERDS" is not compromised;

3) That ERDS Operating Procedures and/or incorporated features within the ERDS design restrict the instrument type to meet the requirements of the Electronic Recording Delivery Act of 2004;

4) That a disciplined and structured process is established to monitor the effectiveness of security controls for the ERDS;

5) That a signed Memorandum of Understanding between clients and the County Recorder is in place and on file;

6) That an ERDS assignment of responsibility or delegation be in the form of a duty statement or a contractual agreement;

7) That ERDS access is controlled by assignment of a role-based access control system defining specific levels of access;

8) Those individuals with secure access to an ERDS have submitted fingerprint image to the Department of Justice for a state and federal criminal record check and have been cleared by the ERDS Program prior to engaging in that role. In addition, have signed the Acknowledgement of Responsibilities (ERDS Form# 0012) and understand their responsibilities as stated on the form;

9) That the ERDS Program is notified when an individual that is engaged in an ERDS role changes that role, by the submission of the Change of ERDS Role (ERDS Form#0008); and

10) ERDS procedures are in place for handling and responding to any reportable incident of know or suspected security violation(s).

Appendix C FEE SCHEDULE

System Administration Fee
A County Recorder establishing an ERDS shall pay for the direct cost of regulation and oversight by the ERDS Program. A System Administration Fee developed in consultation with interested County Recorders has been established to meet this requirement.

A County Recorder shall enter into a Memorandum of Understanding with the ERDS Program, before system certification, agreeing to the computed System Administration Fee and annually thereafter by an addendum to the Memorandum of Understanding. On an annual basis, the System Administration Fee shall be computed based on the following:

- The ERDS Program's estimated annual costs;
- The number of counties participating in the System Administration Fee;
- The total documents recorded and filed by the participating counties, as reported to the Office of the Insurance Commissioner pursuant to Section 27296 of the Government Code, for the previous calendar year;
- A percentage figure will be calculated, by dividing the total documents recorded per participating county, by the total documents recorded for all participating counties;
- The percentage figure is applied to the estimated annual costs of the ERDS Program to arrive at each participating county's System Administrative Fee.

Note: Failure to pay the County's proportionate share of the System Administration Fee, operating under a certified ERDS, shall result in the suspension of the System Certificate of Operation.

Vendor Fees
The ERDS Program shall charge non-refundable fees directly to a vendor seeking certification as a Vendor of ERDS Software. The fees are:

- Vendor of ERDS Software Certification $500.00
- Renewal Certification $300.00

Fingerprint Processing Fees
For an individual designated a secure access role the fees for fingerprint processing are:

- Fingerprint Live Scan & Fingerprint Card (State) $32.00
- Fingerprint Live Scan & Fingerprint Card (Federal) $17.00

Other Fees
Other fees that may be charged, by the ERDS Program, include the following:

- Returned (bounced) Check $10.00
- Copy of Certificate $10.00
- Copy of Document(s) .30 per page

Note: Fees are payable in the form of a check or money order. All fees are processed before completion of the request.

Appendix D ACRONYMS AND DEFINITIONS

Acronym, Term or Phrase	Definitions
Agent	A representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter who has entered into a contract with a County Recorder, and, assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software. (Refer to the definition of "Vendor (or Developer)" later in this section.)
Approved Escrow Company	An escrow company approved pursuant to California Code of Regulations, Title 2, Division 7, Chapter 6, Article 3, D, List of Approved Companies and Facilities, Section 20639.
Attorney General	The Attorney General of the State of California.
Authorized Access	A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.
Authorized Submitter	A party and his/her employees that has entered into a contract with a County Recorder, and, assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software.
CCISDA	California County Information Services Directors Association
CCR	California Code of Regulations
Certificate Authority	A certificate authority that issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.
CFE	Certified Fraud Examiner
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
Computer Security Auditor	(1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vender of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.

Acronym, Term or Phrase	Definitions
County Recorder	A public official responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.
County Recorder Designee	A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
Developer	Refer to Vendor of ERDS Software.
Digital Electronic Record	A record containing information that is created, generated, sent, communicated, received, or stored by electronic means, but not created in original paper form.
Digital Signature	A set of electronic symbols attached to, included in, or logically associated with one or more Type 1 and/or Type 2 instruments, inclusive of information related to and intended for association with the Type 1 and/or Type 2 instruments, that is the result of a process, or processes, designed and employed for the purpose of verifying the integrity, accuracy, or authenticity of the Type 1 and/or Type 2 instruments with related information. For the purpose of an ERDS, a digital signature is generated by encrypting the hash value of an ERDS payload.
Digitized Electronic Record	A scanned image of the original paper document.
DOJ	The California Department of Justice
Electronic Signature of the Notary	A field, or set of fields, containing information about the electronic signature of the notary who notarized a Type 1 or Type 2 Instrument.
ERDA	Electronic Recording Delivery Act of 2004.
ERDS	Electronic Recording Delivery System – An ERDS Program certified system to deliver digitized Type 1 and/or Type 2 Instruments to a County Recorder, and, when applicable, return to the Authorized Submitter.
ERDS Account Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure accounts, assign roles, and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
ERDS Payload	An electronic structure designed for the purpose of delivering Type 1 or Type 2 instruments to a County Recorder via an ERDS. The structure is also used to return, and, when applicable, Type 1 or Type 2 instruments to an Authorized Submitter via an ERDS.
ERDS Program	The program within DOJ designated by the Attorney General to certify, implement, regulate, and monitor an ERDS.

Acronym, Term or Phrase	Definitions
ERDS Server	Computer hardware, software, and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the application software associated with an ERDS. The ERDS Server includes software for encrypting, decrypting, hashing, submitting, and, when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.
ERDS System Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings, and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
FIPS	Federal Information Processing Standard
GIAC	Global Information Assurance Certification
GSNA	GIAC Systems and Network Auditor
HMAC	Hash Message Authentication Code
Incident	An event that may have compromised the safety or security of an ERDS.
Instrument	A “Type 1” instrument is defined to mean an instrument affecting a right, title, or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. Individuals given role-based privileges for a Type 1 instrument shall be fingerprinted. A “Type 2” instrument is defined to mean an instrument of reconveyance, substitution of trustee, or assignment of deed of trust. Type 2 instruments may be delivered as digitized electronic records or digital electronic records. Individuals given role-based privileges for a Type 2 only instrument shall not be fingerprinted.
Lead County	The County Recorder in a Multi-County ERDS responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.
Live Scan	A DOJ system used for the electronic submission of applicant fingerprints. This system is outside of the ERDS Program.
Logged	An auditable ERDS event.
Logical	The way data or systems are organized. For example, a logical description of a file is that it is a collection of data stored together
MAC	Message Authentication Codes
Multi-County	An ERDS application where County Recorders collaborate and make use of a single ERDS serving multiple counties.
NIST	National Institute of Standards and Technology
Non-Substantive Modification	A change that does not affect the functionality of an ERDS.
ORI	Originating Agency Identifier

Acronym, Term or Phrase	Definitions
Physical Access	Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls
Public Entity	Includes the State, the Regents of the University of California, a county, city, district, public authority, public agency, any other political subdivision or public corporation in the State, and federal government entities.
PKI	A Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority, which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with.
Reportable	An incident that has resulted in the compromise of the safety or the security of an ERDS and shall be reported to the ERDS Program.
RSA	A public-key encryption technology developed by Rivest, Shamir and Adelman (RSA). The RSA algorithm has become the de facto standard for industrial-strength encryption especially for data sent over the Internet.
Role	A security mechanism, method, process or procedure that defines specific privileges dictating the level of access to an ERDS.
SANS Institute	Systems and Network Security Institute
Secure Access	A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator who is authorized to configure hardware, software, and network settings; 4) an ERDS Account Administrator who is authorized to configure accounts, assign roles, and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return submitted ERDS payloads.
Security Testing	An independent security audit by a Computer Security Auditor, including, but, not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.
SHA	Secure Hash Algorithm
Source Code	A program or set of programs, readable and maintainable by humans, translated or interpreted into a form that an ERDS can execute.
Source Code Materials	Source Code Materials must include, but, are not limited to: 1) a copy of all source code that implements ERDS functionality; 2) a copy of the compiler needed to compile the ERDS source code in escrow; 3) Instructions for installation and use of the ERDS source code compiler; and 4) Instructions that facilitate reviews, modification and/or recompiling the source code.
Sub-County	The collaborating County Recorder(s) in a Multi-County ERDS operation.

Acronym, Term or Phrase	Definitions
Substantive Modification	A change that affects the functionality of an ERDS.
TLS	Transport Layer Security (formerly known as Secure Socket Layer)
Uniform Index Information	Information collected by a County Recorder in the recording process. Every Type 1 and Type 2 Instruments delivered through an ERDS shall be capable of including uniform index information. The County Recorder shall decide on the content of uniform index information.
User	A person who uses a computer to access, submit, retrieve, or, when applicable, return an ERDS payload.
Vendor of ERDS Software (or Developer)	A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resources used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.
Workstation	A computer used to connect to, and interact with, an ERDS.