Electronic Recording Delivery System
Computer Security Auditor Handbook

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

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. The oversight responsibility is met by audits and local inspections of an ERDS. The primary process for monitoring the effectiveness of security controls is a computer security audit conducted by a Computer Security Auditor with a valid Certificate of Approval issued by the ERDS Program, pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 18, Articles 1 through 9.

This handbook describes the criteria and procedures to obtain approval as a Computer Security Auditor, which authorizes the individual to contract with a County Recorder(s) to perform the duties of a Computer Security Auditor. The Certificate of Approval does not guarantee employment as an approved Computer Security Auditor. 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.

An individual applying for approval as a Computer Security Auditor may obtain the Computer Security Auditor Approval application 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 COMPUTER SECURITY AUDITOR CRITERIA AND APPLICATION PROCESS

A Computer Security Auditor approval is granted based on an individual's significant experience and having no disqualifying offense(s) based on a state and federal criminal record check from fingerprint submission.

(A) Application Submission - Any individual or company/employer seeking Computer Security Auditor approval shall complete and submit, on an individual basis, an Application for Computer Security Auditor Approval (ERDS Form #0002) to the ERDS Program.

(1) The application shall be dated and signed declaring under penalty of perjury that under the laws of the State of California all the foregoing information and all information submitted with the application is true, correct and complete, and that a false or dishonest answer to any question shall be grounds for denial or subsequent termination of approval.

In addition, the individual shall attest to the fact that he or she is not an Authorized Submitter, Agent of an Authorized Submitter, or Vendor of ERDS Software as defined in the CCR, Title 11, Division 1, Chapter 18, Article 2.

(2) Selecting Geographical Location(s) - Check the geographical location(s) on the application, which shall identify the area the individual is interested in providing auditing services. The locations are:

(a) Northern California: Amador, Alpine, Butte, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Nevada, Placer, Plumas, Sacramento, Shasta, Sierra, Siskiyou, Solano, Sonoma, Sutter, Tehama, Trinity, Yolo, Yuba.

(b) Central California: Alameda, Calaveras, Contra Costa, Fresno, Inyo, Kern, Kings, Madera, Mariposa, Merced, Mono, Monterey, San Benito, San Francisco, San Joaquin, San Luis Obispo, San Mateo, Santa Clara, Santa Cruz, Stanislaus, Tulare, Tuolumne.

(c) Southern California: Imperial, Los Angeles, Orange, Riverside, San Bernardino, Santa Barbara, San Diego, Ventura.

(d) All.

(3) Significant Experience - Submit documentation with the Application for Computer Security Auditor Approval (ERDS Form #0002), as follows, to demonstrate that the individual has met the significant experience criteria required for approval as a Computer Security Auditor:

(a) A copy of their Certified Internal Auditor certification from the Institute of Internal Auditors for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 year of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(b) A copy of their Certified Information Systems Auditor certification from the Information Systems Audit and Control Association for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 year of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(c) A copy of their Certified Fraud Examiner certification from the Association of Certified Fraud Examiners for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, **or**

(d) A copy of their Certified Information Systems Security Professional certification from the International Information Systems Security Certification Consortium for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, **or**

(e) A copy of their Global Information Assurance Certification from the SysAdmin, Audit, Networks Security Institute for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies.

(4) Proof of fingerprint submission as outlined in Section 3 of this handbook.

SECTION 3 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. In addition, a Computer Security Auditor shall be granted approval and issued a Certificate of Approval, by the ERDS Program, before entering into a contract(s) with a County Recorder(s) to perform the duties of a Computer Security Auditor.

An individual seeking approval as a Computer Security Auditor 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) Attach the contributing agency copy of the Request for the Live Scan Service form (BCIA 8016ERDS), as proof of fingerprint submission, to the Application for Computer Security Auditor Approval (ERDS Form #0002); and

(3) Retain the applicant copy of the Request for Live Scan Service form (BCIA 8016ERDS), should proof of fingerprint submission be needed at a later date.

(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 a fingerprinting service site 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 following as an attachment to the Application for Computer Security Auditor Approval (ERDS Form #0002):

(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 can not be fingerprinted 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 provide the following as an attachment to the Application for Computer Security Auditor Approval (ERDS Form #0002):

(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; 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.)

(B) Fingerprint Status

Once the fingerprints are submitted, the DOJ processes 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 ERDS Program shall proceed with processing the application.

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

If the individual has a criminal record with a disqualifying offense(s), the individual shall be notified by the ERDS Program, in writing, that they are denied approval as a Computer Security Auditor.

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 elect to reapply by the submission of fingerprint images for a state and federal criminal record check according to the submission methods outlined in this section and an ERDS application. 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 the 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 application, if applicable.

(C) Subsequent Arrest and/or Disposition Notification

When an individual has been subsequently arrested and/or disposition, 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 a criminal record with a disqualifying offense(s), the ERDS Program shall send a termination letter, within ten business days

If the individual does not receive a letter within ten business days, then it was determined that the individual had no disqualifying offense(s) and shall continue their 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 Computer Security Auditor may notify the ERDS Program. If the Computer Security Auditor wants to continue as an approved Computer Security Auditor, the individual shall submit fingerprints for a state and federal criminal record check according to the submission methods outlined in this section.

SECTION 4 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 individual, 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 post the Auditor's contact information and geographical location(s) interested in auditing on the ERDS web page at http://oag.ca.gov/erds, and send the following to the approved individual:

(a) An approval letter; and

(b) An ERDS Certificate of Approval, which authorizes the individual to contract with a County Recorder(s) to perform the duties of a Computer Security Auditor. The Certificate of Approval shall remain in effect for three years unless a termination is issued based on a subsequent arrest or the Computer Security Auditor withdraws their approval status. (Refer to Section 3 and 6 of this handbook.)

(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 individual with a written explanation and instructions on resubmission. It is the responsibility of the individual to ensure that the application is 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.

If no response is received by the 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 be deemed to 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 records, or to protect homeowners from financial harm.

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

SECTION 5 RENEWAL OF APPROVAL

The approval of a Computer Security Auditor, as issued by the ERDS Program, shall remain in effect for a period of three years from the date of issuance. The three-year period has been established to assure that the approved individual has maintained a qualified status and continues to meet all criteria and possesses sufficient experience required to conduct computer security audits.

In order to be considered a renewal, the Certificate of Approval shall be renewed prior to the expiration date. If the certificate holder fails to comply with the renewal requirements, their Certificate of Approval shall expire by operation of the law at midnight on the expiration date stated on the certificate, which shall render the certificate invalid and all computer security auditing services shall cease.

If an application for renewal is received after the expiration date, the application shall not be considered a renewal and shall be returned to the individual with a cover letter outlining the process for initial application submission, which includes submission of fingerprint images. (Refer to Section 2 of this handbook.)

(A) The certificate holder shall submit to the ERDS Program, a completed Application for Computer Security Auditor Approval (ERDS Form #0002), indicating renewal, which shall be dated and signed declaring under penalty of perjury that under the laws of the State of California all the foregoing information, and all information submitted with the application is true, correct, and complete, and that a false or dishonest answer to any question shall be grounds for denial or subsequent termination or suspension of approval.

In addition, the individual shall attest to the fact that he or she is not an Authorized Submitter, Agent of an Authorized Submitter, or Vendor of ERDS Software as defined in the CCR, Title 11, Division 1, Chapter 18, Article 2.

(B) The geographical location(s) on the application for Computer Security Auditor Approval (ERDS Form #0002), in which they are interested in providing auditing services, shall be checked. The locations are:

(1) Northern California: Amador, Alpine, Butte, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Nevada, Placer, Plumas, Sacramento, Shasta, Sierra, Siskiyou, Solano, Sonoma, Sutter, Tehama, Trinity, Yolo, Yuba.

(2) Central California: Alameda, Calaveras, Contra Costa, Fresno, Inyo, Kern, Kings, Madera, Mariposa, Merced, Mono, Monterey, San Benito, San Francisco, San Joaquin, San Luis Obispo, San Mateo, Santa Clara, Santa Cruz, Stanislaus, Tulare, Tuolumne.

(3) Southern California: Imperial, Los Angeles, Orange, Riverside, San Bernardino, Santa Barbara, San Diego, Ventura.

(4) All.

(C) Submit documentation with the Application for Computer Security Auditor Approval (ERDS Form #0002), as follows, to demonstrate that the individual has met the significant experience criteria required for approval as a Computer Security Auditor:

(1) A copy of their Certified Internal Auditor certification from the Institute of Internal Auditors for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 year of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(2) A copy of their Certified Information Systems Auditor certification from the Information Systems Audit and Control Association for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 year of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(3) A copy of their Certified Fraud Examiner certification from the Association of Certified Fraud Examiners for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(4) A copy of their Certified Information Systems Security Professional certification from the International Information Systems Security Certification Consortium for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies; **or**

(a) A copy of their Global Information Assurance Certification from the SysAdmin, Audit, Networks Security Institute for which they are in good standing attached to the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies.

(D) Proof of fingerprint submission is not required for a renewal.

(E) The ERDS Program shall process the application in accordance with the Application Review process as outlined in Section 4 of this handbook.

SECTION 6 WITHDRAWAL OF APPROVAL

A certificate holder choosing to withdraw their approval status shall notify the ERDS Program. All ERDS auditing services, by the certificate holder, shall cease as of the Cease of Operation/Service date noted on the Application for Withdrawal (ERDS Form #0010). Submission to the ERDS Program and the withdrawal process are as follows:

(A) The Computer Security Auditor shall submit to the ERDS Program an Application for Withdrawal (ERDS Form #0010), 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.

The withdrawing Computer Security Auditor shall cease all ERDS auditing services as of the Cease of Operation/Service date noted on the withdrawal application. The withdrawal request shall render the Certificate of Approval invalid.

If at a later date, the withdrawing certificate holder wishes to have his or her Certificate of Approval reinstated, the individual shall complete the process for initial application submission, which includes submission of fingerprint images.

(B) Upon receipt of withdrawal request, the ERDS Program shall send an acknowledgement letter to the requestor and removed the Computer Security Auditor’s information from the list of approved Computer Security Auditors on the ERDS web page.

SECTION 7 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 copies pertain to his or her application submission. 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 8 APPENDICES

A Geographical Location(s)
B Fee Schedule
C Acronyms and Definitions

Appendix A GEOGRAPHICAL LOCATION(s)

THESE COUNTIES ARE USED TO SELECT GEOGRAPHICAL LOCATION(S) INTERESTED IN AUDITING:

Northern California:

Amador, Alpine, Butte, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Nevada, Placer, Plumas, Sacramento, Shasta, Sierra, Siskiyou, Solano, Sonoma, Sutter, Tehama, Trinity, Yolo, Yuba.

Central California:

Alameda, Calaveras, Contra Costa, Fresno, Inyo, Kern, Kings, Madera, Mariposa, Merced, Mono, Monterey, San Benito, San Francisco, San Joaquin, San Luis Obispo, San Mateo, Santa Clara, Santa Cruz, Stanislaus, Tulare, Tuolumne.

Southern California:

Imperial, Los Angeles, Orange, Riverside, San Bernardino, Santa Barbara, San Diego, Ventura.

All

Appendix B 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 by county is applied to the estimated annual costs of the ERDS Program to arrive at each participating county's figure.

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 nonrefundable 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 C 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.
Substantive Modification	A change that affects the functionality of an ERDS.

Acronym, Term or Phrase	Definitions
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.