California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Table of Contents

Article 1. Scope

§ 100. Scope
§ 101. ERDS Documentation

Article 2. Definitions

§ 200. Definitions

Article 3. Fees

§ 300. Vendor of ERDS Software Fees
§ 301. System Administration Fee

Article 4. Fingerprinting and Criminal Record Checks

§ 400. Fingerprinting and Criminal Record Checks
§ 401. Role-Based Fingerprinting Requirement

Article 5. Baseline Requirements and Technology Standards
§ 500. Basis for the Baseline Technology and Requirements Standards
§ 501. Standards and Guidelines
§ 502. Instrument Type
§ 503. Operating Procedures
§ 504. System Implementation
§ 505. Payload Structure, Content and Usage
§ 506. Uniform Index Information
§ 507. Electronic Signature of a Notary
§ 508. Security Requirements for Data Integrity
§ 509. Security Requirements for Payload Protection
§ 510. Security Requirements for Computer Workstations
§ 511. Security Requirements for Computer Media
§ 512. ERDS Identification Security Requirements
§ 513. ERDS Authentication Security Requirements
§ 514. ERDS Role-Based Security Requirements
§ 515. ERDS Server Security Requirements
§ 516. ERDS Security Requirements for Network Security
§ 517. Physical Security
§ 518. Auditable Events, Incidents and Reporting

§ 519. Proprietary Software
§ 520. Escrow Requirements
§ 521. Deposit of Software Modification into Escrow
§ 522. Letter of Deposit
§ 523. Integrity of Materials
§ 524. Retention and Disposition of Materials
§ 525. Access to Materials
§ 526. Escrow Agreement State Non-responsibility

Article 6. Electronic Recording Delivery System Certification

§ 600. Establishing an ERDS
§ 601. Certification Application Procedure
§ 602. Substantive Modification Application Procedure
§ 603. Non-Substantive Modification Procedure
§ 604. Approval of Application
§ 605. Incomplete Application
§ 606. Denial of Application
§ 607. Change of County Recorder
§ 608. Change of Physical and/or Mailing Address and/or Contact Information for a County Recorder
§ 609. Addition or Deletion of Individuals Assigned an ERDS Role that Requires Fingerprinting
§ 610. Expiration of Certification
§ 611. Withdrawal of Certification
§ 612. Request for Replacement of Certificate and/or Documents

Article 7. Computer Security Auditor Approval

§ 700. DOJ Computer Security Auditor Application Procedure
§ 701. Approval of Application
§ 702. Incomplete Application
§ 703. Denial of Application
§ 704. Expiration of Approval
§ 705. Renewal of Approval
§ 706. Withdrawal of Approval
§ 707. Request for Replacement of Certificate and/or Documents

Article 8. Vendor of Electronic Recording Delivery System Software Certification

§ 800. Certification Application Procedure
§ 801. Fingerprinting of Vendor Employees and/or Vendor Contract Employees
§ 802. Approval of Application
§ 803. Incomplete Application
§ 804. Denial of Application
§ 805. Expiration of Certification
§ 806. Renewal of Certification

§ 807. Withdrawal of Certification
§ 808. Request for Replacement of Certificate and/or Documents

Article 9. Audits and Oversight

§ 900. Security Audits
§ 901. Audit Report Format
§ 902. Local Inspection
§ 903. Incident Reporting
§ 904. Suspension and Termination of Certification
§ 905. Notification
§ 906. Reconsideration

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 1. Scope

§ 100. Scope

(a) This chapter shall be known as Department of Justice (DOJ) regulations for Electronic Recording Delivery System (ERDS) and is referred to as these regulations.

(b) These regulations establish guidelines, procedures, and standards following the enactment of the Electronic Recording Delivery Act (ERDA) of 2004, which authorizes a County Recorder, upon approval by resolution of the board of supervisors and system certification by the ERDS Program, to establish an ERDS for the delivery, and, when applicable, return of specified digitized and digital electronic records, subject to specified conditions, including system certification, regulation, and oversight by the ERDS Program.

(c) These regulations may not be construed to administer the processes or procedures relating to the business of a County Recorder.

(d) These regulations do not address prevention for tampering or fraudulent documents prior to transmitting into or after retrieving from an ERDS.

Authority cited: Sections 27391(a), 27391(b), 27392(a), 27393(a), 27393(b), 27393(c), 27396(a), 27399(a) Government Code.
Reference: Sections 27391(a), 27391(b), 27392(a), 27393(a), 27393(b), 27393(c), 27396(a), 27399(a) Government Code.

§ 101. ERDS Documentation

Documentation submitted to the ERDS Program shall be exempt from disclosure pursuant to the Information Practices Act of 1977, Civil Code Section 1798 et seq.

Authority cited: Sections 27393(c), 27394(d) Government Code.
Reference: Sections 27393(c), 27394(d) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 2. Definitions

§ 200 Definitions

(a) For the purposes of this Chapter, the following definitions shall apply throughout of all the articles in the Chapter:

(1) "Agent" means 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 to deliver, and, when applicable, return of Type 1 and 2 instruments (excludes Type 2 instruments only) in a secure access role and/or Type 2 instruments via an ERDS. An Agent may not be a DOJ approved Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software.

(2) "Approved Escrow Company" means 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.

(3) "Attorney General" means the Attorney General of the State of California.

(4) "Authorized Access" means 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 level of access does not require fingerprinting.

(5) "Authorized Submitter" means a party and his/her employees that has entered into a contract with a County Recorder to deliver, and, when applicable, return of Type 1 and 2 instruments in a secure access role (excludes Type 2 instruments only) or Type 1 instruments only; and/or Type 2 instruments via an ERDS. An Authorized Submitter may not be a DOJ approved Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.

(6) "Certificate Authority" means a certificate authority issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS implementation. Certificate authorities also validate digital certificates presented as proof of identity.

(7) "Computer Security Auditor" means: 1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits, and 2) A role assigned by the County Recorder to DOJ approved computer security personnel who are authorized

to review transaction logs and conduct tests on computer security mechanisms. A DOJ approved Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software. This role requires fingerprinting. A DOJ approved Computer Security Auditor shall be issued a certificate by the ERDS Program.

(8) "County Recorder" means a public official (as authorized pursuant to subdivision (a) of Section 27391) 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.

(9) "County Recorder Designee" means a Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return of submitted ERDS payloads. A County Recorder Designee may not be a DOJ approved Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.

(10) "Developer" has the same meaning as "Vendor".

(11) "Digital Electronic Record" means a record containing information that is created, generated, sent, communicated, received, or stored by electronic means, but not created in original paper form.

(12) "Digital Signature" means a set of electronic symbols attached to, included in, or logically associated with one or more digital electronic records and/or digitized electronic records, inclusive of information related to and intended for association with the digital electronic records and/or digitized electronic records, that is the result of a process, or processes, designed and employed for the purpose of verifying the integrity, accuracy or authenticity of the digital electronic records and/or digitized electronic records with related information. For the purpose of an ERDS, a digital signature is generated by encrypting the hash value of an ERDS payload.

(13) "Digitized Electronic Record" means a scanned image of the original paper document.

(14) "DOJ" means The California Department of Justice.

(15) "Electronic Signature of the Notary" means a field, or set of fields, containing information about the electronic signature of the notary who signed, sealed or stamped a digital electronic record or digitized electronic record.

(16) "ERDA" means Electronic Recording Delivery Act of 2004.

(17) "ERDS" means an ERDS Program certified Electronic Recording Delivery System to deliver digitized electronic records and/or digital electronic records to a County

Recorder for recording, and, when applicable, may return to the party requesting recording.

(18) "ERDS Account Administrator" means 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 DOJ approved Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.

(19) "ERDS Server" means 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 returning ERDS payloads. It also includes storage media for ERDS payloads in the process of being delivered to the County Recorder or being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that ERDS server functions can be isolated from other server functions, as evidenced by audit.

(20) "ERDS Payload" means an electronic structure designed for the purpose of delivering digital electronic records or digitized electronic records to a County Recorder via an ERDS. The structure is also used to return, when applicable, digital electronic records or digitized electronic records to an Authorized Submitter via an ERDS.

(21) "ERDS Program" means the program within DOJ designated by the Attorney General to certify, implement, regulate and monitor an ERDS.

(22) "ERDS System Administrator" means a secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software and network settings. An ERDS System Administrator may not be a DOJ approved Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.

(23) "FIPS" means Federal Information Processing Standard.

(24) "HMAC" means Hash Message Authentication Code.

(25) "Incident" means an event that may have compromised the safety or security of an ERDS.

(26) "Instrument" means: (1) A Type 1 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; and (2) A Type 2 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

(27) "Lead County" means 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.

(28) "Live Scan" means a DOJ system used for the electronic submission of applicant fingerprints. This system is outside of the ERDS Program.

(29) "Logged" means an auditable ERDS event.

(30) "Logical" means 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.

(31) "MAC" means message authentication codes.

(32) "Multi-County" means an ERDS application where County Recorders collaborate and make use of a single ERDS servicing multiple counties.

(33) "NIST" means National Institute of Standards and Technology.

(34) "Non-substantive Modification" means a change that does not affect the functionality of an ERDS. Non-substantive modifications include, but are not limited to, the following: 1) Day-to-day administration of ERDS accounts, roles or cryptographic keys; 2) Hardware maintenance that does not affect the functionality of ERDS and does not involve the complete replacement of an ERDS server; 3) The off-loading of ERDS server logs to long-term storage; 4) Updating anti-malware software with the most up-to-date releases; 5) Updating operating system software with the most up-to-date patches and hot-fixes; 6) Maintaining backups for software and data; and 7) The addition and/or deletion of roles, whether or not fingerprinting or notification to the ERDS Program is required.

(35) "ORI" means Originating Agency Identifier.

(36) "Physical Access" means 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.

(37) "PKI" means a Public Key Infrastructure which 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.

(38) "Reportable" means an incident that has resulted in the compromise of the safety or security of an ERDS and shall be reported to the ERDS Program.

(39) "RSA" means 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.

(40) "Role" means a security mechanism, method, process or procedure that defines specific privileges dictating the level of access to an ERDS.

(41) "Secure Access" means 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 DOJ approved 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 of submitted ERDS payloads.

(42) "Security Testing" means an independent security audit by a DOJ approved Computer Security Auditor, including, but not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.

(43) "SHA" means Secure Hash Algorithm.

(44) "Source Code" means a program or set of programs, readable and maintainable by humans, translated or interpreted into a form that an ERDS can execute.

(45) "Source Code Materials" means, but is not limited to, all of the following: 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.

(46) "Sub-County" means the collaborating County Recorder(s) in a Multi-County ERDS operation.

(47) "Substantive Modification" means a change that affects the functionality of an ERDS. Substantive modifications include, but are not limited to the following: 1) Changes to source code that lead to new or different functional behaviors; 2) Changes to call signatures in source code interfaces to purchased components; 3) Changes of data

structures or structural database object; 4) Changes that require modification of deployment procedures; 5) A new version of a compiler that requires source code changes in order to compile existing source code error and warning free; 6) Changes to purchased components or components that are part of software libraries; 7) Relocation of an ERDS server to a different network segment; 8) Changing an ERDS server from single-purpose to multi-purpose; 9) Changing an ERDS server from Single-county to Multi-County; 10) Hardware maintenance involving the complete replacement of an ERDS server; 11) Software maintenance releases that correct, perfect, enhance or otherwise affect the functionality of ERDS.

(48) "TLS" means Transport Layer Security.

(49) "Uniform Index Information" means information collected by a County Recorder in the recording process. Every digital electronic record and digitized electronic record delivered through an ERDS shall be capable of including uniform index information. The County Recorder shall decide on the content of uniform index information.

(50) "User" means a person who uses a computer to access, submit, retrieve, or return if applicable, an ERDS payload, or otherwise access, operate or modify an ERDS.

(51) "Vendor (or Developer)" means 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 jurisdictions for establishing an ERDS. A Vendor of ERDS Software may not be a DOJ approved 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.

(52) "Workstation" means a computer used to connect to, and interact with, an ERDS.

Authority cited: Sections 27390(b), 27391(b), 27393(a), 27393(b), 27393(c), 27395(f) Government Code.
Reference: 27390(b), 27391(b), 27393(a), 27393(b), 27393(c), 27395(f) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 3. Fees

§ 300. Vendor of ERDS Software Fees

(a) The ERDS Program fees for certification of a Vendor of ERDS Software are as follows:

(1) Initial certification by the ERDS Program is $500.

(2) Renewal certification by the ERDS Program is $300.

Authority cited: Sections 27393(c), 27397(b) Government Code.
Reference: Sections 27393(c), 27397(b) Government Code.

§ 301. System Administration Fee

(a) 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 the interested County Recorders, has been established to meet this requirement.

(b) On an annual basis, the System Administration Fee shall be computed based on all of the following:

(1) DOJ's estimated annual costs.

(2) The number of counties participating in the System Administration Fee.

(3) 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.

(4) A percentage figure will be calculated by dividing the total documents recorded per participating county by the total documents recorded for all participating counties.

(5) The percentage figure by county is applied to the estimated annual costs of the ERDS Program to arrive at each participating county's figure.

(c) 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.

Authority cited: Sections 27393(c), 27397(a) Government Code.
Reference: Sections 27393(c), 27397(a) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 4. Fingerprinting and Criminal Records Checks

§ 400. Fingerprinting and Criminal Record Checks

(a) Individuals assigned an ERDS role that requires fingerprinting by the County Recorder shall submit fingerprint images and all related information to DOJ for the purpose of obtaining information as to the existence and nature of a record of state and federal level convictions and arrests or whether the applicant was released on bail or his own recognizance pending trial.

(b) If the state or federal criminal records contain a conviction of a felony, or a misdemeanor related to theft, fraud, or a crime of moral turpitude, or a pending criminal charge for all of these crimes shall be justification for denial to an individual to serve in an ERDS role that requires fingerprinting. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction pursuant to Government Code section, 27395 (a), irrespective of a subsequent order under section 1203.4 of the Penal Code. All other state or federal criminal records containing a felony or misdemeanor conviction involving dishonesty, fraud or deceit, "moral turpitude" [People v. Castro (1985) 38 Cal. 3d 301], including pending charges, shall be justification for denial to an individual to serve in an ERDS role that requires fingerprinting.

(c) The DOJ shall respond to the ERDS Program for criminal offender record information as delineated in subdivision (l) of section 11105 of the Penal Code.

(d) The ERDS Program shall deliver written notification of an individual's ineligibility for access to an ERDS to the individual, his or her known employer, the DOJ approved Computer Security Auditor, and the County Recorder.

(e) The ERDS Program shall request subsequent arrest notification service, pursuant to Section 11105.2 of the Penal Code for individuals assigned an ERDS role that requires fingerprinting.

(f) If the ERDS Program is notified of a subsequent arrest, the individual, their employer and the County Recorder shall be notified within 10 business days of the individual's ineligibility for access to an ERDS, if applicable.

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

(1) There may be occasions when an employee of the County Recorder or of an Authorized Submitter, who was previously approved for an ERDS role that requires fingerprinting, changes roles and/or agencies.

(2) Re-fingerprinting is not required if an employee of either the County Recorder or of an Authorized Submitter changes roles 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 now submits to multiple counties. Re-fingerprinting is not required if an individual accepts employment with another ERDS operation and is designated an ERDS role that requires fingerprinting. However, a Change of ERDS Role form #ERDS 0008 shall be completed consistent with procedures outlined in these regulations.

(3) Proof of fingerprint submission can be met as follows:

(A) Electronic fingerprint submissions. A notarized applicant copy of the Request for Live Scan Services form # BCII 8016 shall be provided as proof of fingerprint submission. If a notarized copy cannot be provided, the individual shall be fingerprinted.

(B) Manual fingerprint submissions. If an individual initially used the manual method of fingerprinting, the individual shall be fingerprinted.

Authority Cited: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b), 27395(c), 27395(d) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b), 27395(c), 27395(d) Government Code.

§ 401. Role Based Fingerprinting Requirement

(a) The following ERDS roles require the submission of fingerprints to DOJ, and require DOJ clearance based on the criminal records check, prior to the individual serving in the role:

(1) Agent or 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 to deliver, and return Type 1 and 2 instruments (excludes Type 2 instruments only) in a secure access role and/or Type 2 instruments via an ERDS. An Agent may not be a DOJ approved Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software.

(2) Authorized Submitter and his/her employees is a party that has entered into a contract with a County Recorder to deliver, and return Type 1 and 2 instruments in a secure access role (excludes Type 2 instruments only) or Type 1 instruments only; and/or Type 2 instruments via an ERDS. An Authorized Submitter may not be a DOJ approved

Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.

(3) Computer Security Auditor who is: 1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits, and 2) A role assigned by the County Recorder to DOJ approved computer security personnel who are authorized to review transaction logs and conduct tests on computer security mechanisms. A DOJ approved Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.

(4) County Recorder Designee with a secure access role assigned by the County Recorder to retrieve and return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software.

(5) ERDS Account Administrator with 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 DOJ approved Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software.

(6) ERDS System Administrator with a secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software and network settings. An ERDS System Administrator may not be a DOJ approved Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software.

(7) An individual who is authorized physical access to an ERDS server with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.

(8) Vendor (or Developer) 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 jurisdictions for establishing an ERDS. A Vendor of ERDS Software may not be a DOJ approved Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator or County Recorder Designee.

Authority Cited: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b), 27395(c), 27395(d) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b), 27395(c), 27395(d) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 5. Baseline Requirements and Technology Standards

§ 500. Basis for the Baseline Requirements and Technology Standards

(a) To meet the intent of the ERDA, the minimum standards and guidelines established within this article are based on information security "best practices" designed to offer a layered security approach through the use of the following security objectives:

(1) Availability (of systems and data for intended use only). Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users, i.e, accessible and usable upon demand. This objective protects against intentional or accidental attempts to either perform unauthorized deletion of data or otherwise cause a denial of service or data.

(2) Integrity (of system and data). Integrity has two facets:

(A) Data integrity (the property that data has not been altered or destroyed in an unauthorized manner while in storage, during processing, or while in transit), or

(B) System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

(3) Confidentiality (of data and system information). Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals, entities or processess. Confidential protection applies to data in storage, during processing, and while in transit.

Authority cited: Sections 27390(a), 27391(b), 27392, 27393(a), 27393(b), 27393 (c), 27397.5(a) Government Code.
Reference: Sections 27390(a), 27391(b), 27392, 27393(a), 27393(b), 27393 (c), 27397.5(a) Government Code.

§ 501. Standards and Guidelines

Standards and guidelines contained in these regulations are based on FIPS, NIST Special Publication 800-88, (Draft Special Publication Dated February 3, 2006), and other references. Newly developed ERDS shall conform to the most current version of references cited. Deployed ERDS shall be made to conform within 2 years of an update, revision or replacement of a

reference cited. The ERDS Program shall issue a directive when conformance is required within a period of less than 2 years.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 502. Instrument Type

(a) The ERDA refers to two types of instruments that may be delivered, and returned as digital electronic records and/or digitized electronic records. For the purposes of ERDS, these instruments are classified as follows:

(1) Type 1 is 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.

(2) Type 2 is 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

(b) ERDS shall be designated as Type 1 or Type 2 or Type 1 and 2. The delivery and, when applicable, return of these instrument types through an ERDS shall meet the requirements specified in these regulations.

Authority cited: Sections 27391(b), 27393(a), 27393(b), 27393 (c), 27397.5(a) Government Code.
Reference: Sections 27391(b), 27393(a), 27393(b), 27393 (c), 27397.5(a) Government Code.

§ 503. Operating Procedures

(a) The County Recorder shall have ERDS operating procedures prepared, maintained and followed that explain the proper operation, management, administration, content restrictions and use of their ERDS.

(b) The County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type and content to meet the requirements of the ERDA.

(c) ERDS operating procedures shall be sufficient for a DOJ approved Computer Security Auditor to conduct a computer security audit.

Authority cited: Sections 27390(a), 27391(b), 27392, 27393(a), 27393(b), 27393(c), 27394(c), 27397.5(a), 27397.5(c) Government Code.
Reference: Sections 27390(a), 27391(b), 27392, 27393(a), 27393(b), 27393(c), 27394(c), 27397.5(a), 27397.5(c) Government Code.

§ 504. System Implementation

(a) ERDS may consist of hardware, software, storage media and network connections that securely exchange messages and data. The hardware, software and storage media shall be designated by the County Recorder establishing the ERDS and shall be included in system certifications, audits, local inspections and reviews.

(b) ERDS shall be designated as "Single-County" or "Multi-County". Single-County ERDS shall be dedicated to serving a single county. Multi-County ERDS shall serve more than one county as established by mutual agreement among County Recorders.

(c) An Authorized Submitter may be granted access to more than one ERDS; however, access to each ERDS shall remain under management control of the County Recorder establishing the ERDS.

(d) ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

(e) ERDS shall protect the confidentiality and integrity of digital electronic records and/or digitized electronic records during the process of transmission and storage.

(f) ERDS capable of returning digital electronic records and/or digitized electronic records shall meet the requirements established within these regulations.

Authority cited: Sections 27392, 27393(a), 27393(b), 27393(c), 27397(a), 27397.5(c), 27397.5(d) Government Code.
Reference: Sections 27392, 27393(a), 27393(b), 27393(c), 27397(a), 27397.5(c), 27397.5(d) Government Code.

§ 505. Payload Structure, Content and Usage

(a) All ERDS for either Type 1 or Type 2 instruments shall contain an ERDS payload structure. An ERDS payload structure does not restrict the content within a digital electronic record and/or digitized electronic record. A County Recorder shall list any restrictions on content in each contract with an Authorized Submitter. At a minimum, the ERDS payload structure shall contain a component for all of the following:

(1) Uniform Index Information.

(2) One or more digital electronic records or digitized electronic records.

(3) Information about the electronic signature of a notary.

(b) Each ERDS payload will be used to generate the Digital Signature of the individual preparing the ERDS payload. When ERDS payloads are being prepared for delivery to a County Recorder, the Digital Signature shall be of the Authorized Submitter. When ERDS payloads are being returned to an Authorized Submitter through ERDS, the Digital Signature shall be of the County Recorder Designee.

(c) ERDS payloads may be used to deliver a file format acceptable to the County Recorder.

(d) ERDS payloads submitted by an Authorized Submitter shall be retrievable by a County Recorder Designee.

(e) Multiple digital electronic records or digitized electronic records within the same payload is allowed; however, Type 1 and Type 2 instruments may not be included in the same ERDS payload.

Authority cited: Sections 27392(b), 27393(a), 27393(b), 27393(c), Government Code.
Reference: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 506. Uniform Index Information

A digital electronic record or digitized electronic record delivered through an ERDS shall be capable of including uniform index information in the ERDS payload. The County Recorder shall decide on the content of uniform index information.

Authority cited: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 507. Electronic Signature of a Notary

(a) ERDS payloads shall be capable of including information about the electronic signature of the notary regardless of how the electronic signature of a notary is affixed by the notary according to other applicable laws. When a signature is required to be accompanied by a notary's seal or stamp, that requirement is satisfied if the electronic signature of the notary contains all of the following:

(1) The name of the notary.

(2) The words "Notary Public".

(3) The name of the county or other administrative district of a state where the bond and oath of office of the notary are filed.

(4) The sequential identification number assigned to the notary, if given.

(5) The sequential identification number assigned to the manufacturer or vendor of the notary's physical and/or electronic seal, if available.

Authority cited: Sections 27391(e), 27392(b), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(e), 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 508. Security Requirements for Data Integrity

(a) All ERDS for either Type 1 or Type 2 instruments shall assure submitted documents do not contain content that draws data or images from sources external to the digital electronic record and/or digitized electronic record, including, but not limited to: viruses, worms, Trojan Horses, spyware, adware, ActiveX components, java script, java components, HTML encoded hyperlinks, and any other executable software.

(b) Active content detected by anti-malware shall be removed as soon as it is detected. Active content that cannot be removed shall be disabled.

Authority cited: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 509. Security Requirements for Payload Protection

(a) All ERDS for either Type 1 or Type 2 instruments shall employ encryption, both in transmission and storage, until decrypted by the intended recipient to protect the confidentiality of ERDS Payloads. Once decrypted by the intended recipient, the security of the contents shall become the responsibility of the intended recipient. Two payload encryption algorithms are approved for ERDS:

(1) The RSA Algorithm using a minimum key-length of 1024 bits, and

(2) The Advanced Encryption Algorithm using a minimum key-length of 128 bits as defined in FIPS 197, Advanced Encryption Standard (publication date November 26, 2001).

(b) All ERDS for either Type 1 or Type 2 instruments shall use hashing to protect the integrity of ERDS payloads. The hash function approved for ERDS payloads is the Secure Hash Algorithm defined in FIPS 180-2, Secure Hash Standard (publication date December 1, 2003), using a message digest size of at least 224 bits.

(c) All ERDS for either Type 1 or Type 2 instruments shall use Digital Signatures to assure the authenticity of ERDS payloads. The signing function approved for ERDS payloads is the RSA algorithm, using a minimum key-length of 1024 bits.

(d) All ERDS for either Type 1 or Type 2 instruments shall use a Public Key Infrastructure (PKI) established by the County Recorder to ensure all ERDS users are uniquely identified and to protect the integrity and authenticity of ERDS payloads. The public/private key-pair shall

constitute the user's PKI identity credentials. Cryptographic modules used for generating encryption keys shall meet the requirements of Security Level 2 defined in FIPS 140-2, Security Requirements for Cryptographic Modules (publication date May 25, 2001, supersedes FIPS PUB 140-1 January 11, 1994).

(e) ERDS for Type 1 instruments: The private key in the pair shall be issued to the user and employed to create digital signatures, both for use during login and for assuring the integrity of ERDS payloads. The public key shall be used to authenticate the user during login and to verify the integrity and authenticity of ERDS payloads.

(f) ERDS for Type 2 instruments: The private key in the pair shall be issued to the user and employed to create digital signatures and for assuring the integrity of ERDS payloads. The public key shall be used to authenticate the user and to verify the integrity and authenticity of ERDS payloads.

(g) ERDS for Type 1: Authentication shall consist of two factors: the user ID and password associated with an approved user account and the user's PKI identity credentials.

(h) ERDS for Type 2 instruments: Authentication shall be based on the user's PKI identity credentials.

(i) All ERDS for either Type 1 or Type 2 instruments: Resources and means for establishing a PKI shall be at the discretion of the County Recorder, but commercially available certificate authorities, if employed, shall be on the list of certification authorities approved by the California Secretary of State.

Authority cited: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 510. Security Requirements for Computer Workstations

(a) All ERDS that serve either Type 1 or Type 2 instruments: The County Recorder shall ensure that all endpoints are secure. As such, workstations used to submit, retrieve, or return if applicable ERDS payloads are protected from unauthorized use and access. As a minimum, workstations shall meet all of the following requirements:

(1) Anti-malware software configured to start on system boot-up.

(2) Operating system software with the most up-to-date patches and hot-fixes.

(3) Host based Firewall configured to restrict inbound and outbound connections.

(b) For Type 1 instruments only, installed applications shall be limited to the purpose of performing the necessary operational needs of the recording process as defined by the County Recorder.

(c) The County Recorder shall include provision (a) and (b) as a mandatory requirement in all contracts with Authorized Submitters whom shall ensure that an Agent, if any, complies with these regulations. The contents of the contract provision are subject to audit.

Authority cited: Sections 27391(b), 27392, 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(b), 27392, 27393(a), 27393(b), 27393(c) Government Code.

§ 511. Security Requirements for Computer Media

(a) ERDS Payloads and encryption keys for either Type 1 or Type 2 instruments shall be encrypted when stored on storage media. The encryption employed for protecting ERDS payloads and encryption keys in storage shall conform to the standards for transmitting ERDS payloads.

(b) Fixed and removable disks for either Type 1 or Type 2 instruments shall be sanitized as defined in NIST Special Publication 800-88, (Draft Special Publication Dated February, 2006), Guidelines for Media Sanitization prior to reallocating ERDS hardware or storage media to other purposes.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 512. ERDS Identification Security Requirements

(a) ERDS that serve both Type 1 and Type 2 instruments shall be required to meet the additional identification security requirements required for Type 1 instruments as follows:

(1) User accounts may be implemented as part of a network authentication and authorization system available to the County Recorder, as an integral part of an ERDS server, or by other means at the discretion of the County Recorder as long as all of the following requirements are met:

(A) Each ERDS user shall be uniquely identified.

(B) Shared user accounts and identity credentials shall be prohibited.

(C) User IDs shall either be based on the verified name of the user or a pseudonym approved by the County Recorder.

(D) User accounts shall be associated with ERDS roles.

Authority cited: Sections 27392, 27393(a), 27393 (b), 27393(c) Government Code.
Reference: Sections 27392, 27393(a), 27393 (b), 27393(c) Government Code.

§ 513. ERDS Authentication Security Requirements

(a) ERDS that serve both Type 1 and Type 2 instruments shall be required to meet all of the additional authentication security requirements required for Type 1 instruments as follows:

(1) The standard for electronic authentication shall employ a token containing a cryptographic key, for example a digital certificate, issued to the user and a password associated with the user ID.

(2) Authentication assurance shall meet Level 3 or higher, as defined by the NIST Special Publication 800-63 [April 2006 Version 1.0.2 (publication updated) (document original released date June 2004)].

(3) The token methods described by the NIST may be used, provided that authentication assurance Level 3 or higher, as defined by the NIST Special Publication 800-63, is achieved.

(b) Password creation, protection, maintenance, processing and handling shall adhere to the Password Policy contained in the California Counties Best Policies for the Countywide Information Security Program.

Authority cited: Sections 27392, 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392, 27393(a), 27393(b), 27393(c) Government Code.

§ 514. ERDS Role-Based Security Requirements

(a) ERDS that serve both Type 1 and Type 2 instruments shall be required to meet all of the additional role-based security requirements for Type 1 instruments as follows:

(1) ERDS access shall be controlled by the County Recorder using a role-based access control system. Textual disclaimers or verbal disclaimers alone shall not be sufficient to control access to digital electronic records and digitized electronic records under the control of an ERDS. The role-based access control system shall control all of the following characteristics:

(A) Whether or not a session may be established with an ERDS.

(B) What ERDS Payloads will be displayed.

(C) Whether or not ERDS Payloads may be submitted, retrieved and/or returned.

(D) Whether Type 1 instruments or Type 2 instruments may be included within an ERDS payload.

(2) The County Recorder shall also be responsible for controlling the assignment of user accounts and identity credentials. User accounts and identity credentials shall be

issued to the person, and a role shall be assigned to control transactions performed under that user account. The security system shall be capable of controlling this electronic access based on the roles authorized at the time a user successfully logs into an ERDS.

(3) Shared user accounts may not be issued. At no time shall more than one person be authorized access to an ERDS using a single ERDS user account or set of identity credentials. Each person shall be uniquely identified.

(4) If a user's status changes so that access to ERDS is no longer required, the user's ERDS account and identity credentials shall be disabled and revoked for the purposes of ERDS. ERDS user accounts and identity credentials may not be transferable.

(5) Identity credentials shall be recognized across ERDS provided that the County Recorders involved have consented, by mutual agreement, to recognize the credentials. The details of the agreements shall be at the discretion of the County Recorders; however, the agreement shall be made part of the ERDS operating procedures of all County Recorders who are party to the agreement.

(6) The security system of a Multi-County ERDS shall be capable of controlling access based on the county to which ERDS payloads are to be delivered.

(7) With the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls, persons granted physical access to an ERDS server shall be subject to fingerprinting, but may not be assigned a login role and may not be granted access to ERDS payloads unless authorized by the County Recorder.

(8) An Authorized Submitter shall be limited to those privileges granted by the County Recorder. The Authorized Submitter is prohibited from submitting ERDS payloads on behalf of another Authorized Submitter, or Agent, unless the details of the agreement are specified in contracts with the County Recorder. Regardless of the details of the agreement, shared user accounts may not be issued.

(9) An Agent named in more than one contract shall be required to indicate which Authorized Submitter is represented in a transaction.

Authority cited: Sections 27391(b), 27392, 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(b), 27392, 27393(a), 27393(b), 27393(c) Government Code.

§ 515. ERDS Server Security Requirements

(a) ERDS that employ one or more servers that serve both Type 1 and Type 2 instruments shall be required to meet all of the additional server security requirements for Type 1 instruments as follows:

(1) Separate physical servers dedicated to performing ERDS server functions are not required provided that ERDS server functions can be isolated from other server functions, as evidenced by audit.

(2) ERDS shall employ an ERDS proxy server.

(3) The web/proxy server shall do all of the following:

(A) Establish secure Internet sessions.

(B) Authenticate user ID and password credentials.

(C) Transfer and/or relay ERDS requests received via authenticated secure Internet sessions to the ERDS server.

(D) Be physically and logically separated from the ERDS server.

(4) Web/Proxy servers may not execute an ERDS functionality except as described above.

(5) The ERDS server shall communicate via secure sessions through the web/proxy server when interoperating via the Internet. As a minimum, sessions between the web/proxy server and ERDS server shall be protected using a secure protocol. Direct logins from the Internet to an ERDS server shall be prohibited.

(6) The ERDS server shall run ERDS applications software, store ERDS payloads, authenticate ERDS credentials, and control ERDS access, based on assigned roles and log ERDS transactions.

(7) ERDS servers shall be configured to prevent unauthorized access, modification or use.

(8) At a minimum, servers shall be hardened according to the standards established by the County Recorder. The County Recorder shall ensure that all county servers used for ERDS are "hardened" according to one of the following checklists or guidelines:

(A) NIST Security Configuration Checklists as defined in SP 800-70 (publication date May 2005) designed for the product.

(B) Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.

(C) Security guidelines available from industry standard sources such as the Computer Emergency Response Team Coordination Center or the System and Network Security Institute.

(9) All county servers used for ERDS shall have a host-based file integrity checking system configured to alert security staff of an operating system file change to the ERDS server and have anti-malware software installed and operating to protect the server.

Authority cited: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.

§ 516. ERDS Security Requirements for Network Security

(a) ERDS that serve both Type 1 and Type 2 instruments shall be required to meet all of the additional network security requirements for Type 1 instruments as follows:

(1) ERDS transactions via a network shall be protected using encryption.

(2) Prior to beginning a login sequence, a secure connection shall be established in order to protect passwords. ERDS may not employ "basic" or Hypertext Transport Protocol referred to commonly as "HTTP" authentication to transmit passwords. Secure connections shall be terminated if the authenticated user logs out or after a preset timeout limit of not more than 30 minutes, whichever occurs first.

(3) The standard for establishing secure connection is the TLS protocol as described in NIST Special Publication 800-63, Electronic Authentication Guideline (publication date April 2006, Version 1.0.2). As a minimum, 128-bit encryption shall be used to establish secure TLS sessions, as described in FIPS 197 (Publication Dated November 26, 2001), "Advanced Encryption Standard".

(4) ERDS shall employ MAC to assure the authenticity of encrypted ERDS packets. Each MAC shall conform to the standard defined in FIPS 198, "The Keyed-Hash Message Authentication Code (HMAC)" (publication date April 8, 2002).

(5) The County Recorder shall ensure digital certificates are available to establish secure connections between users and the web/proxy server, and between the web/proxy server and ERDS server.

(6) Network security controls shall be implemented to prevent unauthorized network traffic from reaching ERDS components.

(7) ERDS components shall be protected from unauthorized network access. Network perimeter security controls shall be implemented to prevent unauthorized network traffic from reaching ERDS components. At a minimum, network devices shall do all of the following:

(A) Employ stateful packet inspection.

(B) Block unauthorized connections by limiting connection attempts addressed to ERDS components to those necessary for ERDS operation.

(C) Be designed and configured to fail "closed" rather than open.

(D) Detect possible intrusions and, if a possible intrusion is detected, alert security staff and take action to prevent the intrusion.

Authority cited: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.

§ 517. Physical Security

(a) With the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls, including fingerprinting, the site housing the ERDS server shall be protected from unauthorized physical access. The server shall be locked in a manner as to prevent unauthorized physical access.

(b) The County Recorder shall ensure precautions are employed to protect the ERDS server, software and data from theft, damage and/or unauthorized access or use. Precautions may be defined in County Recorder ERDS operating procedures or may be established by mutual agreement between the County Recorder and the entity housing the ERDS server.

(c) As a minimum, ERDS operating procedures and/or mutual agreements shall provide for the following:

(1) All requests for physical access to an ERDS server are subject to disapproval by the County Recorder. For an ERDS involving a shared, multi-purpose server, the County Recorder may not have overall authority to approve physical access; however, the County Recorder shall retain disapproval authority in an agreement involving shared multi-purpose servers.

(2) Persons who are authorized physical access to an ERDS server require fingerprinting.

(3) An inventory that accounts for all keys, whether physical or electronic used for locking and unlocking physical access to an ERDS server, software and/or data shall be completed at least every 90 calendar days.

(4) During audits, the DOJ approved Computer Security Auditor shall be allowed to inspect all access requests and inventory reports that occurred within the 2-year period prior to the start of an audit.

(5) During local inspections, ERDS Program staff shall be allowed to inspect all access requests and inventory reports that occurred within the 2-year period prior to the start of a local inspection.

Authority cited: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(a), 27393(a), 27393(b), 27393(c) Government Code.

§ 518. Auditable Events, Incidents and Reporting

(a) Auditable ERDS events shall be logged for purposes of audit, local inspection and review, incident response, and reporting. Auditable events may be logged using automated and/or manual processes. Logs shall be safely stored and maintained in a manner that ensures their availability for (1) a period of at least 24 months, or (2) at least 1 computer security audit, whichever occurs later.

(b) The County Recorder shall establish ERDS operating procedures for handling and responding to an incident as defined by these regulations.

(c) Incident reporting shall comply with provisions contained in this Chapter.

(d) All of the following are auditable ERDS events for both Type 1 or Type 2 instruments, unless otherwise stated, that shall be logged, and when applicable, processed only as an incident or processed as an incident and reported.

(1) For Type 1 only, login successes and failures.

(2) For Type 1 only, sessions starts and ends.

(3) For Type 1 only, session time-outs.

(4) For Type 1 only, ERDS payload submittals, retrievals and returns.

(5) For Type 1 only, ERDS transaction not conducted within a preset timeout limit. Criteria for setting the timeout shall be established by the County Recorder; however, the maximum preset timeout limit is 30 minutes. This is an incident.

(6) For Type 1 only, ERDS session is terminated within a preset timeout limit without receiving a logout command. This is an incident.

(7) For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas; or any user attempting to use ERDS software and/or interfaces in a non-ERDS manner. This is an incident and shall be reported if fraud is suspected.

(8) Use of expired or revoked credentials. This is an incident and shall be reported if fraud is suspected.

(9) For Type 1 only, privilege elevation. This is an incident and shall be reported.

(10) For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session. This is an incident and shall be reported if fraud is suspected.

(11) For Type 1 only, unauthorized user gaining access to an ERDS server or ERDS payload storage area. This is an incident and shall be reported.

(12) Any user gaining access using expired or revoked credentials. This is an incident and shall be reported.

(13) Authentication fails.

(14) Authentication failure on consecutive login attempts. This is an incident.

(15) Auditable events overwrite other logged events. This is an incident and shall be reported if intrusion is suspected.

(16) Auditable events cannot be logged. This is an incident.

(17) Logs consume 95% or more of the storage space allocated for logging. This is an incident.

(18) Logs cannot be safely stored. This is an incident.

(19) For Type 1 only, ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not. This is an incident only if not authorized and shall be reported.

(20) For Type 1 only, hardware or software configuration changes. This is an incident only if not authorized and shall be reported.

(21) Unique name of the ERDS payload. This is an incident only if out of sequence.

(22) Dates and times the ERDS payload was submitted, retrieved or returned. This is an incident only if the dates and times are not current.

(23) Identity of the individual, who submitted, retrieved or returned the ERDS payload. This is an incident only if not authorized.

(24) Name of the organization that the individual represented while submitting, retrieving or returning the ERDS payload**.** This is an incident only if suspended.

(25) For Type 1 only, a transmission failure.

(26) For Type 1 only, a storage failure.

(27) A decryption failure. This is an incident.

(28) A hash failure. This is an incident.

(29) A validity check failure. This is an incident.

(30) Type 1 or Type 2 instrument submitted unencrypted. This is an incident and shall be reported.

(31) Type 1 instrument submitted as a Type 2 instrument or vice versa. This is an incident and shall be reported if fraud is suspected.

(32) Type 1 instrument submitted via an Authorized Access ERDS. This is an incident and shall be reported if fraud is suspected.

(33) For Type 1 only, unauthorized digital electronic record in a digitized electronic record, or vice versa. This is an incident and shall be reported if fraud is suspected.

(34) Unauthorized components that draw data or images from sources external to the digital electronic record or digitized electronic record. This is an incident and shall be reported if intrusion is suspected.

(35) Unauthorized transactions submitted via ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2. This is an incident and shall be reported if fraud is suspected.

(36) For Type 1 only, server failures, including, but not limited to, hardware, software, and network component failures, that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(37) Events for which security staff are alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected.

(38) For Type 1 only, unauthorized changes to the ERDS operational configuration. This is an incident and shall be reported if fraud or intrusion is suspected.

(39) For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(40) For Type 1 only, events for which security staff are alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected. This is an incident and shall be reported if intrusion is suspected.

(41) For Type 1 only, unauthorized changes to the ERDS operational configuration. This is an incident and shall be reported.

(42) Inability to obtain and employ up-to-date anti-malware software.

(43) Inability to obtain and employ cryptography, including hashing, encryption and decryption. This is an incident and shall be reported.

(44) Use of either compromised or weak encryption algorithms. This is an incident and shall be reported.

(45) For Type 1 only, discovery of newly published vulnerability existing on a certified ERDS. This is an incident and shall be reported.

(46) Discovery of susceptibility to newly published exploit. This is an incident and shall be reported.

(47) Inability to obtain and employ the most up-to-date patches and hot-fixes.

(48) Unauthorized access or changes to storage media, and improper sanitization of storage media. This is an incident and shall be reported if compromise is suspected.

(49) Any other event that compromises the safety or security of an ERDS. This is an incident and shall be reported.

Authority cited: Sections 27392(a), 27393, 27394 Government Code.
Reference: Sections 27392(a), 27393, 27394 Government Code.

§ 519. Proprietary Software

(a) The DOJ approved Computer Security Auditor may not be required to conduct a source code review on any software identified as proprietary by the Vendor of ERDS Software unless such software affects the safety and security of ERDS.

(b) Prior to conducting a source code review, the County Recorder shall ensure all of the following:

(1) The County Recorder has agreed to allow the Vendor of ERDS Software to include proprietary source code as part of the ERDS.

(2) The Vendor of ERDS Software has identified proprietary source code as part of the ERDS.

(3) The DOJ approved Computer Security Auditor advises the County Recorder that the safety and security of ERDS cannot be verified without a source code review.

(4) The DOJ approved Computer Security Auditor shall agree to abide by confidentiality requirements of the Vendor of ERDS Software.

(5) The Vendor of ERDS Software shall agree that the DOJ approved Computer Security Auditor shall reveal any results of the source code review, conclusions as to the safety and security of ERDS, and recommendations, in the audit report.

(6) The County Recorder, DOJ approved Computer Security Auditor and Vendor of ERDS Software shall all agree on methods for including the results, conclusions and recommendations about proprietary source code reviews made by the DOJ approved Computer Security Auditor in the audit report.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394 Government Code.

§ 520. Escrow Requirements

(a) ERDS source code materials shall be placed into an approved escrow facility when an ERDS is developed for a County Recorder. For each submission, the materials placed in escrow shall be sufficient to maintain ERDS of every County Recorder that employs those source code materials. Source code materials, include, but are not limited to, all of the following:

(1) A copy of all source code materials 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.

(4) Instructions that facilitate source code reviews, modification and/or recompiling the ERDS source code.

(b) A County Recorder shall select an escrow company from the current Secretary of State's list as obtained from the County's Board of Supervisors.

(c) Source code materials shall be submitted to an approved escrow company for placement in the escrow facility. The content of source code materials shall be in a form, and include the tools and documentation, to allow complete and successful restoration of an ERDS in its production/operational environment with confirmation by a verification test by qualified personnel using only this content.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 521. Deposit of Software Modification into Escrow

Substantive modifications shall require updates to source code materials in escrow. Prior to being used to deliver Type 1 or Type 2 instruments in an ERDS, all source code changes or

modifications shall be submitted into escrow in the same manner and under the same conditions in which the source code materials were originally placed in escrow.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 522. Letter of Deposit

(a) Within a timeframe established by the County Recorder of a submission of original, changed or modified source code to an approved escrow facility, the developer shall notify, in writing, each affected County Recorder that the source code has been placed in escrow. The letter of deposit shall include a description of submitted materials sufficient to distinguish them from all other submissions. The letter of deposit shall state all of the following:

    (1) That all source code materials are included in the deposit.

    (2) The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow.

    (3) The escrow company, its officers, and directors, may not hold or exercise a direct or indirect financial interest(s) in the developer or the County Recorder.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 523. Integrity of Materials

No person having access to ERDS source code materials shall interfere with or prevent the escrow representative from monitoring the security and integrity of the ERDS source code materials.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 524. Retention and Disposition of Materials

Records maintained by the escrow company pursuant to these regulations and other applicable law shall be retained for the term of the escrow agreement. The escrow agreement shall provide for the disposition of source code materials in the event the escrow agreement terminates.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 525. Access to Materials

Escrow agreements shall allow for access to ERDS source code materials by a DOJ approved

Computer Security Auditor hired for the purpose of conducting computer security audits.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394(e) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394(e) Government Code.

§ 526. Escrow Agreement State Non-responsibility

(a) Neither the Attorney General nor the State of California shall be responsible for the fees claimed by the developer, the County Recorder, or the escrow company to establish the escrow contract.

(b) Neither the Attorney General nor the State of California is a party to the agreement and may not incur a liability for the actions of the parties involved in the escrow agreement.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 6. Electronic Recording Delivery System Certification

§ 600. Establishing an ERDS

(a) A County Recorder may establish an ERDS upon approval by the Board of Supervisors and system certification by the ERDS Program.

(b) A County Recorder establishing an ERDS shall include in the County's ERDS a secure method for accepting for delivery, and, when applicable, return of a digital electronic record or digitized electronic record that has been defined as an Instrument within this chapter.

(c) A County Recorder establishing an ERDS shall be responsible for overall safety and security of an ERDS.

(d) A County Recorder establishing an ERDS shall assign responsibility by contract or agreement to all authorized submitters whom shall ensure that an Agent, if any, complies with these regulations.

(e) A County Recorder shall be responsible for ensuring an ERDS meets the requirements of these regulations.

(f) A County Recorder shall enter into a contract with a DOJ approved Computer Security Auditor for the purpose of meeting the audits and oversight requirements as contained within this Chapter. The terms of the contract shall include that a DOJ approved Computer Security Auditor may not be required to conduct a source code review on software identified as proprietary by the Vendor of ERDS Software, if any, unless such software affects the safety and security of ERDS.

(g) A County Recorder shall be required, 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.

(h) The County Recorder shall be responsible for administering an ERDS, and establishing and following ERDS policies and procedures that include all of 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 disclaimers or verbal disclaimers alone

shall not be sufficient to control access to digital electronic records and digitized electronic records under the control of an ERDS.

(2) Maintain a list of users and roles authorized to access and operate the ERDS and informing the ERDS Program of role changes for those individuals requiring fingerprinting.

(3) Ensure users with roles authorized to access and operate the ERDS understand and sign the Acknowledgement of Responsibilities form # ERDS 0012 and that a copy is maintained for review during audits and local inspections.

(4) The County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type and content to meet the requirements of the ERDA.

Authority cited: Sections 27390, 27391(a), 27391(b)**,** 27392, 27393(a), 27393(b), 27393(c), 27394(a), 27394(c), 27394(f), 27396, 27397.5(a) Government Code.
Reference: Sections 27390, 27391(a), 27391(b)**,** 27392, 27393(a), 27393(b), 27393(c), 27394(a), 27394(c), 27394(f), 27396, 27397.5(a) Government Code.

§ 601. Certification Application Procedure

(a) A County Recorder wanting, either in his or her official capacity or by delegation of responsibility, to establish an ERDS for the delivery, and, when applicable, return of a digital electronic record or digitized electronic record shall contact the ERDS Program and request an ERDS Certification application.

(b) A County Recorder may apply for the initial certification of an ERDS operating as either a Single-County or Multi-County operation and shall designate as either a Type 1 or Type 2 or a Type 1 and 2 operation. An ERDS may not be implemented prior to receipt of DOJ's approval of the application.

(1) A County Recorder applying for the initial certification of an ERDS operating as a Single-County ERDS shall comply with all of the following:

(A) Submit an Application for System Certification form # ERDS 0001A to the ERDS Program, which shall be dated and signed declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(B) Submit a copy of the County Resolution to establish an ERDS as approved by the Board of Supervisors.

(C) Submit a copy of the proof of escrow letter of deposit.

(D) Submit a copy of the Vendor of ERDS Software contract, if any. If internal resources are being used to develop an ERDS in lieu of a vendor, it shall be stated in the County Resolution granting establishment of an ERDS.

(E) Submit a copy of the County's contract with a DOJ approved Computer Security Auditor.

(F) Submit a copy of the successful initial system audit report conducted by a DOJ approved Computer Security Auditor.

(G) Submit proof of fingerprint submission for individuals designated as having a role that requires fingerprinting.

(H) Submit a signed and dated Statement of Understanding form # ERDS 0011 declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(2) A County Recorder designated as the Lead County applying for the initial certification of an ERDS operating as a Multi-County ERDS shall comply with the following:

(A) Submit an Application for System Certification form # ERDS 0001A to the ERDS Program, which shall be dated and signed declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(B) Submit the Lead County's Resolution to establish a Multi-County ERDS as approved by the Board of Supervisors.

(C) Submit a copy of the proof of escrow letter of deposit.

(D) Submit a copy of the Vendor of ERDS Software contract, if any. If internal resources are being used to develop an ERDS in lieu of a vendor, it shall be stated in the County Resolution granting the establishment of an ERDS.

(E) Submit a copy of the Lead County's contract with a DOJ approved Computer Security Auditor.

(F) Submit a copy of the successful initial system audit report conducted by a DOJ approved Computer Security Auditor.

(G) Submit proof of fingerprint submission for individuals designated as having a role that requires fingerprinting.

(H) Submit all Sub-County(ies) documentation as an attachment to the application.

(I) Submit a signed and dated Statement of Understanding form # ERDS 0011 declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(3) A County Recorder applying as a Sub-County during the initial certification of a Multi-County ERDS shall comply with all of the following:

(A) Submit an Application for Sub-County System Certification form # ERDS 0001B to the lead county, which shall be dated and signed declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(B) Submit a copy of the Sub-County's Resolution to participate in a Multi-County ERDS as approved by the Board of Supervisors.

(C) Submit proof of fingerprint submission for individuals designated as having a role that requires fingerprinting.

(D) Submit a signed and dated Statement of Understanding form # ERDS 0011 declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

Authority cited: Sections 27390, 27391(a), 27391(b), 27392, 27393(a), 27393 (b), 27393(c), 27394(a), 27395(b) Government Code.
Reference: Sections 27390, 27391(a), 27391(b), 27392, 27393(a), 27393 (b), 27393(c), 27394(a), 27395(b) Government Code.

§ 602. Substantive Modification(s) Application Procedure

(a) Following initial system certification, a Request for Approval of Substantive Modification(s) form # ERDS 0013, as defined in this Chapter, shall require completion of a modified system audit pertaining to only the components that are proposed to be modified and/or changed in the production environment and shall be performed prior to the provisional activation of the modification and/or change in the ERDS operational environment. This modified system audit shall be completed by a DOJ approved Computer Security Auditor and submitted to the County Recorder. Upon receipt of the successful modified system audit by the County Recorder, the County Recorder may place the substantive modification(s) in the production environment on a provisional basis. Within 15 business days of the provisional implementation, the County Recorder shall apply for approval of the substantive modification(s) in order for DOJ to make a final approval determination status.

(b) Requests for approval of substantive modification(s) shall be submitted to the ERDS Program as follows:

(1) Submit a Request for Approval of Substantive Modification(s) form # ERDS 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) Submit a copy of the proof of escrow letter of deposit.

(3) Submit a copy of the County's contract with a DOJ approved Computer Security Auditor.

(4) Submit a copy of the successful Modified System Audit Report conducted by a DOJ approved Computer Security Auditor.

(c) Requests for approval of substantive modification(s) for adding a Sub-County, the Lead County shall submit to the ERDS program as follows:

(1) A copy of the resolution to participate in the Multi-County ERDS as approved by the board of supervisors.

(2) Submit a copy of the proof of escrow letter of deposit.

(3) Submit a copy of the County's contract with a DOJ approved Computer Security Auditor.

(4) Submit a copy of the successful Modified System Audit Report conducted by a DOJ approved Computer Security Auditor.

(5) Submit the Sub-County's Application for Sub-County System Certification form # ERDS 0001B and required documentation as follows:

(A) Submit a copy of the Sub-County's Resolution to participate in a Multi-County ERDS as approved by the Board of Supervisors.

(C) Submit proof of fingerprint submission for individuals designated as having a role that requires fingerprinting.

(D) Submit a signed and dated Statement of Understanding form # ERDS 0011 declaring under penalty of perjury under the laws of California that all information is true and correct.

Authority cited: Sections 27390, 27391(a), 27391(b), 27392, 27393(a), 27393 (b), 27393(c), 27394(a), 27395(b) Government Code.
Reference: Sections 27390, 27391(a), 27391(b), 27392, 27393(a), 27393 (b), 27393(c), 27394(a), 27395(b) Government Code.

§ 603. Non-substantive Modification Procedure

A non-substantive modification, as defined in this Chapter, does not require a modified system audit; however, it shall be subject to review during audits and local inspections.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394(c) Government Code.

§ 604. Approval of Application

(a) If the application for initial System Certification is approved, the ERDS Program shall deliver the following to the County Recorder.

(1) An Approval Letter.

(2) A System Certification of Operation, which authorizes the County Recorder to operate the ERDS.

(b) If the Request for Approval of Substantive Modification(s) form # ERDS 0013 is approved, the ERDS Program shall deliver an approval letter to the County Recorder to implement the substantive modification and to remove the provisional status.

Authority cited: Sections 27391(a), 27392(a), 27393(a), 27393(c) Government Code.
Reference: Sections 27391(a), 27392(a), 27393(a), 27393(c) Government Code.

§ 605. Incomplete Application

(a) An incomplete Application for System Certification form # ERDS 0001A or Request for Approval of Substantive Modification(s) form # ERDS 0013 shall be returned to the County Recorder with a written explanation for the reason for return and instruction on resubmission. Applications shall be deemed incomplete when:

(1) The application has missing or illegible data.

(2) Supporting documentation, forms, or applicable fees are not included with application.

(3) Proof of fingerprint submission for individuals designated as having a role that requires fingerprinting is not submitted.

(b) The applicant shall have 90 days to respond, after which the application shall be considered denied. The denial may not prohibit the resubmission of an Application for System

Certification form # ERDS 0001A or Request for Approval of Substantive Modification(s) form # ERDS 0013 at a later date.

Authority cited: Sections 27392, 27393(a), 27393(b), 27393(c), 27395(b), 27395(e) Government Code.
Reference: Sections 27392, 27393(a), 27393(b), 27393(c), 27395(b), 27395(e) Government Code.

§ 606. Denial of Application

(a) The Application for System Certification form # ERDS 0001A or Request for Approval of Substantive Modification(s) form ERDS # 0013 may be denied for good cause. Good cause shall be deemed to exist when the applicant does not satisfy the qualifications or system requirements of these regulations, when it is necessary to protect the public interest, protect the integrity of public records, or to protect homeowners from financial harm.

(b) Denied applications shall be returned to the County Recorder with a written explanation for the reason for denial. The denial may not prohibit the resubmission of an Application for System Certification form # ERDS 0001A or Request for Approval of Substantive Modification(s) form # ERDS 0013 at a later date.

Authority cited: Sections 27391(a), 27392 (a), 27393 (a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27392 (a), 27393 (a), 27393(b), 27393(c) Government Code.

§ 607. Change of County Recorder

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

Authority cited: Sections 27391(a), 27392(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27392(a), 27393(a), 27393(b), 27393(c) Government Code.

§ 608. Change of Physical and/or Mailing Address and/or Contact Information for a County Recorder

The County Recorder, either in his or her official capacity or by delegation of responsibility, shall notify the ERDS Program within 30 days by submitting a written notification of the change.

Authority cited: Sections 27391(a), 27392(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27392(a), 27393(a), 27393(b), 27393(c) Government Code.

§ 609. Addition or Deletion of Individuals Assigned an ERDS Role that Requires Fingerprinting

The County Recorder shall submit to the ERDS Program a completed Change of ERDS Role form # ERDS 0008 indicating addition or deletion of County Recorder employees and/or contract employees, Authorized Submitter employees or agents, and Vendor of ERDS Software employees and/or contract employees. The County Recorder shall maintain a list of those individuals and their roles which shall be subject to audit and local inspection.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27395(b) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(b) Government Code.

§ 610. Expiration of Certification

(a) Once issued by the ERDS Program, the certification of the ERDS shall remain in effect within the County Recorder's office for which it is approved without the need for renewal for the life of the ERDS operation in the County unless one of the following occur:

(1) A letter of suspension is issued to the County Recorder.

(2) The County Recorder withdraws from ERDS Certification.

Authority cited: Sections 27391(a), 27392, 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27392, 27393(a), 27393(b), 27393(c) Government Code.

§ 611. Withdrawal of Certification

(a) A County Recorder choosing to withdraw from ERDS Certification shall submit the following:

(1) An Application for Withdrawal form # ERDS 0010 with a date for cease of operation/service, signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(2) Listing of all employees designated as having secure access and/or authorized access.

(3) Listing of all associated agencies and/or business entities designated as having secure access and/or authorized access.

(b) If, at a later date, the County Recorder wishes to participate in the ERDS, all initial steps for System Certification shall be required.

Authority cited: Sections 27391(a), 27392, 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27392, 27393(a), 27393(b), 27393(c) Government Code.

§ 612. Request for Replacement of Certificate and/or Documents

(a) To request a replacement certificate or copies of a document pertaining to an application submission, a County Recorder or his or her designee may submit a Request for Replacement of Certificate and/or Documents form # ERDS 0006, signed and dated declaring under penalty of perjury under the laws of the State of California that the requested certificate and/or documents pertain to his or her application submission.

Authority cited: Sections 27391(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27393(a), 27393(b), 27393(c) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 7. Computer Security Auditor Approval

§ 700. DOJ Computer Security Auditor Application Procedure

(a) An individual requesting approval as a DOJ Computer Security Auditor shall contact the ERDS Program and request the DOJ Computer Security Auditor Approval application.

(b) An individual applying for approval as a DOJ Computer Security Auditor shall comply with all of the following:

(1) Submit an Application for DOJ Computer Security Auditor Approval form # ERDS 0002, 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 this application is true, correct, and complete, and that a false or dishonest answer to a question may 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 these regulations.

(A) Check the geographic locations on the Application for DOJ Computer Security Auditor Approval form # 0002 that they are interested in auditing**.** 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.

(2) Submit documentation with the Application for DOJ Computer Security Auditor Approval form # ERDS 0002 as follows to demonstrate that the individual has met the significant experience criteria required for approval as a DOJ 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 DOJ Computer Security Auditor Approval form # ERDS 0002, 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 DOJ Computer Security Auditor Approval form # ERDS 0002, 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 DOJ Computer Security Auditor Approval form # ERDS 0002 and a completed Attachment to ERDS 0002 Computer Security Auditor Significant Experience Reference(s) form # ERDS 0004 listing reference contacts within the last 5-year period that can verify that the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in the conducting of 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 DOJ Computer Security Auditor Approval form # ERDS 0002 and a completed Attachment to ERDS 0002 Computer Security Auditor Significant Experience Reference(s) form # ERDS 0004 listing reference contacts within the last 5-year period that can verify that the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in the conducting of security testing procedures, and specific experience performing Internet penetration studies, or

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

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

(3) Submit proof of fingerprint submission for each individual seeking approval as a DOJ approved Computer Security Auditor.

Authority Cited: Sections 27390(b), 27393 (b), 27393(c), 27395(a), 27395(b) Government Code.
Reference: Sections 27390(b), 27393 (b), 27393(c), 27395(a), 27395(b) Government Code.

§ 701. Approval of Application

(a) If the application is approved, the ERDS Program shall deliver to the individual all of the following documentation:

(1) An Approval Letter, and

(2) An ERDS Certificate of Approval which authorizes the individual to contract with a County Recorder to perform the duties of a DOJ approved Computer Security Auditor.

(b) The approved DOJ Computer Security Auditor's contact information and geographical interest shall be posted on the ERDS web page.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394, 27395(a) Government Code.
Reference: Sections 27392, 27393(a), 27393(b), 27393(c), 27394, 27395(a) Government Code.

§ 702. Incomplete Application

(a) An incomplete application shall be returned to the applicant with a written explanation for the reason for return, and further instructions on resubmission. An application shall be deemed incomplete when:

(1) The application has missing or illegible data.

(2) Supporting documentation, forms, or applicable fingerprint submission fees are not included with application.

(3) Proof of fingerprinting is not submitted.

(b) The applicant shall have 90 days to respond, after which the application shall be considered denied. The denial may not prohibit the resubmission of an Application for ERDS Computer Security Auditor Approval form # ERDS 0002 at a later date.

Authority cited: Sections 27392, 27393 (a), 27393 (c), 27394(b), 27395(b), 27395(e) Government Code.
Reference: Sections 27392, 27393 (a), 27393 (c), 27394(b), 27395(b), 27395(e) Government Code.

§ 703. Denial of Application

(a) The Application for ERDS Computer Security Auditor Approval form # ERDS 0002 may be denied for good cause. Good cause shall be deemed to exist when the applicant does not satisfy the qualifications or system requirements of this Article, it is necessary to protect the public interest, protect the integrity of records, or to protect homeowners from financial harm.

(b) Denied applications shall be returned to the individual with a written explanation for the reason for denial. The denial may not prohibit the resubmission of an Application for DOJ Computer Security Auditor Approval form # ERDS 0002 at a later date.

Authority cited: Sections 27392, 27393(a), 27393(b), 27393(c), 27394(b), 27395(a) Government Code.
Reference: Sections 27392, 27393(a), 27393(b), 27393(c), 27394(b), 27395(a) Government Code.

§ 704. Expiration of Approval

(a) Once issued by the ERDS Program, the ERDS Certificate of Approval shall remain in effect for a period of 3 years from the date of issuance unless one of the following occurs:

(1) A letter of suspension is issued to the individual.

(2) The individual withdraws their approval status as a DOJ approved Computer Security Auditor.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 705. Renewal of Approval

(a) The ERDS Certificate of Approval shall be renewed prior to expiration in order to remain valid. The certificate holder shall submit an Application for DOJ Computer Security Auditor Approval form # ERDS 0002 indicating renewal.

(b) If the certificate holder fails to comply with the renewal requirements, the certification shall expire by operation of law at midnight on the expiration date stated on the certificate. If an application for renewal is received after the expiration date, the application may not be considered a renewal and shall be returned to the applicant with a cover letter outlining the process for initial approval.

(c) If approved, the ERDS Program shall issue a new ERDS Certificate of Approval.

Authority Cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 706. Withdrawal of Approval

(a) A DOJ approved Computer Security Auditor choosing to withdraw their approval status shall submit an Application for Withdrawal form # ERDS 0010 with a date for cease of operation/service, signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct.

(b) Upon receipt of the Application for Withdrawal form # ERDS 0010, the ERDS Program shall send a written acknowledgement of the request for withdrawal and notification that the auditor's information has been removed from the listing of the DOJ approved Computer Security Auditors posted on the ERDS web page.

(c) If at a later date, a DOJ approved Computer Security Auditor wishes to have his or her approval re-instated, the individual shall complete the initial application process.

Authority cited: Sections 27392, 27393 (a), 27393(c), Government Code.
Reference: Sections 27392, 27393 (a), 27393(c), Government Code.

§ 707. Request for Replacement of Certificate and/or Documents

(a) To request a replacement certificate or copies of a document pertaining to their application submission, a DOJ approved Computer Security Auditor may submit a Request for Replacement of Certificate and/or Documents form # ERDS 0006, signed and dated declaring under penalty of perjury under the laws of the State of California that the requested certificate and/or documents pertain to his or her application submission.

Authority cited: Sections 27393 (a), 27393(c), Government Code.
Reference: Sections 27393 (a), 27393(c), Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 8. Vendor of Electronic Recording Delivery System Software Certification

§ 800. Certification Application Procedure

(a) All vendors of software shall be certified by the ERDS Program prior to entering into contracts with County Recorders for the development of an ERDS.

(b) Individuals applying for certification as a Vendor of ERDS Software shall contact the ERDS Program and request the Vendor of ERDS Software Certification application.

(c) An individual applying for certification as a Vendor of ERDS Software shall comply with all of the following:

(1) Submit an Application for Vendor of ERDS Software Certification form # ERDS 0003, 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 this application is true, correct, and complete, and that a false or dishonest answer to a question may be grounds for denial or subsequent termination or suspension of certification. In addition, the individual shall attest to the fact that the software meets all of the audit and testing requirements as contained in the Baseline Requirements and Technology Standards, and acknowledges that DOJ's issuance of the Vendor of ERDS Software Certificate shall include a "disclaimer" stating that the software is not being approved as to its ability to serve/function in an ERDS operational environment nor that it meets all County Recorder's requirements, only that the vendor has stated that it meets all of the audit and testing requirements as contained in the Baseline Requirements and Technology Standards as of the date of the issued certificate.

(2) Submit documentation with the Application for Vendor of ERDS Software Certification form # ERDS 0003 as follows, to demonstrate that they have met the reference or service agreement required to be certified as a Vendor of ERDS Software:

(A) Provide 3 best references within the last 5 years for software products or development of equivalent technology, complexity and size of an ERDS. At least 1 reference shall be for a project using document-imaging technology. Provide this information on the Attachment to ERDS 0003 Vendor Application Form for Reference(s) form # ERDS 0009, or

(B) Operate as a Vendor with a valid California Master Services Agreement, General Services Agreement, or Master Services Agreement. A copy of the agreement(s) shall include 1 or more of the following Consulting Service categories: Application Development; Information Technology Acquisition Support; Project Management;

Project Planning; Strategic Planning; System Implementation; Migration Planning; Software Development; System Analysis; System Design; System Development; and/or System Integration.

(3) Submit proof of fingerprint submission.

(4) Submit a check or money order for all fees.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27395(b), 27395(e), 27397(b) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(b), 27395(e), 27397(b) Government Code.

§ 801. Fingerprinting of Vendor Employees and/or Vendor Contract Employees

(a) At the time that a certified Vendor of ERDS Software enters into a contract with a County Recorder, the vendor shall provide to the County Recorder proof of fingerprint submission of all vendor employees and/or vendor contract employees to be used in an ERDS development and/or implementation.

(1) An ERDS Acknowledgment of Responsibilities form # ERDS 0012 shall be signed and kept on file for all vendor employees and/or vendor contract employees acknowledging an understanding of his and/or her responsibilities and the statute regarding misuse of the ERDS.

(2) The Vendor of ERDS Software shall notify the County Recorder of any addition or deletion of vendor employees and/or vendor contract employees. The County Recorder shall maintain a list of those individuals and their roles which shall be subject to audit and local inspection. The County Recorder shall submit to the ERDS Program a completed Change of ERDS Role form # ERDS 0008 indicating addition or deletion of vendor employees and/or vendor contract employees.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b) Government Code.

§ 802. Approval of Application

(a) If the application is approved, the ERDS Program shall deliver to the individual all of the following documentation:

(1) An Approval Letter, and

(2) A Vendor of ERDS Software Certificate which authorizes the individual to contract with

a County Recorder as a Vendor of ERDS Software.

Authority Cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 803. Incomplete Application

(a) An incomplete Application for Vendor of ERDS Software Certification form # ERDS 0003 shall be returned to the applicant with a written explanation for the reason for return and further instructions on resubmission. The application shall be deemed incomplete when:

(1) The application has missing or illegible data.

(2) Supporting documentation, forms, or applicable fees are not included with the application.

(3) Proof of fingerprint submission of individuals designated as having a role that requires fingerprinting is not submitted with the application.

(b) The applicant shall have 90 days to respond, after which the application shall be considered denied. The denial may not prohibit the resubmission of an Application for a Vendor of ERDS Software Certification form # ERDS 0003 at a later date.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 804. Denial of Application

(a) The Application for Vendor of ERDS Software Certification form ERDS # 0003 may be denied for good cause. Good cause shall be deemed to exist when the applicant does not satisfy the qualification or system requirements of this Article, it is necessary to protect the public interest, protect the integrity of records, or to protect homeowners from financial harm.

(b) Denied applications shall be returned to the individual with a written explanation for the reason for denial. The denial may not prohibit the resubmission of an Application for Vendor of ERDS Software Certification form # ERDS 0003 at a later date.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27395(a), 27395(b) Government Code.

§ 805. Expiration of Certification

(a) Once issued by the ERDS Program, the Vendor of ERDS Software Certificate shall remain in effect for a period of 3 years from the date of issuance unless one of the following occurs:

(1) A letter of suspension is issued to the individual.

(2) The individual withdraws their certification for Vendor of ERDS Software.

Authority cited: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27392(b), 27393(a), 27393(b), 27393(c) Government Code.

§ 806. Renewal of Certification

(a) A Vendor of ERDS Software Certificate shall be renewed prior to expiration in order to remain valid. The certificate holder shall submit:

(1) An Application for Vendor of ERDS Software Certification form # ERDS 0003 indicating renewal.

(2) A check or money order for the renewal fee.

(b) If the certificate holder fails to comply with the renewal requirements, the certification shall expire by operation of law at midnight on the expiration date stated on the certificate. If an application for renewal is received after the expiration date, the application may not be considered a renewal and shall be returned to the applicant with a cover letter outlining the process for initial certification.

(c) If approved, the ERDS Program shall issue a new Vendor of ERDS Software Certificate.

Authority cited: Sections 27393 (a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393 (a), 27393(b), 27393(c) Government Code.

§ 807. Withdrawal of Certification

(a) A Vendor of ERDS Software choosing to withdraw their certification shall submit the following:

(1) An Application for Withdrawal form # ERDS 0010 with a date for cease of operation/service 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 list of all vendor employees and/or vendor contract employees designated as having a role that requires fingerprinting.

(b) Upon receipt of the Application for Withdrawal form # ERDS 0010, the ERDS Program shall send a written acknowledgement of the request for withdrawal.

(c) If, at a later date, a Vendor of ERDS Software wishes to have his or her certification re-instated, the individual shall complete the initial application process.

Authority cited: Sections 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c) Government Code.

§ 808. Request for Replacement of Certificate and/or Documents

a) To request a replacement certificate or copies of a document pertaining to their application submission, a Vendor of ERDS Software may submit a Request for Replacement of Certificate and/or Documents form # ERDS 0006, signed and dated declaring under penalty of perjury under the laws of the State of California that the requested certificate and/or documents pertains to his or her application submission.

Authority cited: Sections 27391(a), 27393(a), 27393(b), 27393(c) Government Code.
Reference: Sections 27391(a), 27393(a), 27393(b), 27393(c) Government Code.

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 17. Electronic Recording Delivery System
Article 9. Audits and Oversight

§ 900. Security Audits

(a) The ERDS Program has the responsibility for oversight and regulation of an ERDS. This responsibility shall be met by the initial system audit, biennial audit, modified system audit, modified system incident audit and local inspection process.

(b) The primary process for monitoring the effectiveness of security controls shall be a computer security audit conducted by a DOJ approved Computer Security Auditor. A County Recorder shall contract with a DOJ approved Computer Security Auditor in order to meet all ERDS audit requirements. A list of DOJ approved Computer Security Auditors is located on the ERDS web page.

(c) A DOJ approved Computer Security Auditor shall conduct a security audit of an 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) that ERDS have no capability to modify, manipulate, insert, or delete information in the public record.

(1) The facility(ies) of a Type 2 only Authorized Submitter is exempt from a physical security audit when the DOJ approved Computer Security Auditor has validated that all the requirements of these regulations have been met, including certification by the County Recorder and the Attorney General that the method of submission allowed under the system will not permit an Authorized Submitter or its employees and agents, or any third party, to modify, manipulate, insert, or delete information in the public record, maintained by the County Recorder, or information in Type 1 documents which are submitted for electronic recording.

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

(d) The ERDS Initial System Audit is a full system audit and is required to obtain initial system certification. "Initial" is defined as the "first time" application for a certification of an ERDS 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 DOJ approved Computer Security Auditor. 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

form # ERDS 0001A. A successful initial system audit shall be sufficient to meet the 1st year audit requirement and shall include, but is not necessarily limited to, all of the following:

(1) Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.

(2) Demonstration of the proposed system in its intended production/operational environment.

(3) The audit shall show all of the following:

(A) ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.

(B) Transmissions only occur between authorized parties.

(C) Remnants of sessions, transmissions and ERDS payloads are not stored once the user initiating the session and transmitting ERDS payloads has logged out or been disconnected (either physically or logically).

(D) Authorized and unauthorized users are limited in terms of roles assigned to operate the system.

(E) Auditable events are logged correctly.

(F) Known vulnerabilities have been eliminated or mitigated.

(G) The ERDS implementation is not susceptible to published exploits.

(H) ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the ERDA.

(I) ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

(4) Documentation shall include all of the following:

(A) A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the proposed system.

(B) A review of source code, either selected software components or all software.

(C) An inventory of hardware, software and network devices comprising the proposed system.

(D) An inventory of users and roles authorized to access and operate the proposed system.

(E) A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server, and the ERDS servers visible from a non-ERDS workstation or server.

(F) A review of the ERDS operating procedures proposed by the County Recorder.

(G) A review of all security checklists proposed for auditing the ERDS.

(H) A review of contracts with Authorized Submitters.

(I) That the requirements of these regulations are met.

(e) A Biennial Audit and a local inspection are required in alternating years to meet the ongoing oversight of an existing certified Single-County ERDS or a Multi-County ERDS. The biennial audit is a full system audit and shall be performed in the production and operational environment and shall be completed by a DOJ approved Computer Security Auditor and submitted to the County Recorder. A local inspection shall be performed in the alternating years and shall be completed by ERDS Program staff. The County Recorder shall submit a copy of the successful biennial audit report to the ERDS Program. A biennial security audit report shall include, but is not necessarily limited to, all of the following:

(1) Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.

(2) Demonstration of the ERDS in its production/operational environment.

(3) The audit shall show all of the following:

(A) ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.

(B) Transmissions only occur between authorized parties.

(C) Remnants of sessions, transmissions and ERDS payloads are not stored once the user initiating the session and transmitting ERDS payloads has logged out or been disconnected (either physically or logically).

(D) Authorized and unauthorized users are limited in terms of roles assigned to operate the system.

(E) Auditable events are logged correctly.

(F) Known vulnerabilities have been eliminated or mitigated.

(G) The ERDS is not susceptible to published exploits and that the published updates to the standards and guidelines as described in these regulations shall be implemented within two years.

(H) ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the ERDA.

(I) ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

(4) Documentation shall include all of the following:

(A) A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the system.

(B) A review of source code, either selected software components or all software.

(C) An inventory of hardware, software and network devices comprising the system.

(D) An inventory of users and roles authorized to access and operate the system.

(E) A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server, and the ERDS servers visible from a non-ERDS workstation or server.

(F) A review of the ERDS operating procedures established by the County Recorder.

(G) A review of all security checklists established for auditing the ERDS.

(H) A review of contracts with Authorized Submitters.

(I) A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.

(J) A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

(K) That the requirements of these regulations are met.

(f) A Modified System Audit is required to obtain approval for making a substantive modification to an existing certified Single-County ERDS or a Multi-County ERDS. A modified system audit shall pertain to only the components that are proposed to be modified and/or changed in the production environment and shall be performed prior to activating the modification and/or change in the ERDS operational environment. This modified system audit shall be completed by a DOJ approved Computer Security Auditor and submitted to the County Recorder. Upon receipt of the successful modified system audit by the County Recorder, the County Recorder may place the proposed substantive modification in the production environment on a provisional basis. 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 an application for a Request for Approval of Substantive Modification(s) form. A successful modified system audit may not replace the biennial audit requirement. A modified system audit report shall include, but is not necessarily limited to, all of the following:

(1) A Description of Deposit Materials showing that modified source code that has been deposited in escrow with an approved escrow facility.

(2) Demonstration of the ERDS system in its intended production/operational environment.

(3) The audit shall focus on functions of the substantive modification and show all of the following:

(A) ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.

(B) Transmissions only occur between authorized parties.

(C) Remnants of sessions, transmissions and ERDS payloads are not stored once the user initiating the session and transmitting ERDS payloads has logged out or been disconnected (either physically or logically).

(D) Authorized and unauthorized users are limited in terms of roles assigned to operate the system.

(E) Auditable events are logged correctly.

(F) Known vulnerabilities have been eliminated or mitigated.

(G) The ERDS implementation is not susceptible to published exploits.

(H) ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the ERDA.

(I) ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

(4) Documentation shall include all of the following:

(A) A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the proposed system.

(B) A review of source code, either selected software components or all software.

(C) An inventory of hardware, software and network devices comprising the proposed system.

(D) An inventory of users and roles authorized to access and operate the system.

(E) A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server, and the ERDS servers visible from a non-ERDS workstation or server.

(F) A review of the ERDS operating procedures established by the County Recorder.

(G) A review of all security checklists established for auditing the ERDS.

(H) A review of contracts with Authorized Submitters.

(I) A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.

(J) A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

(K) That the requirements of these regulations are met.

(g) A Modified System Incident Audit is required to meet the audit requirement resulting from an incident that compromises the safety or security of an ERDS. Incidents are detailed in the Baseline Technology and Requirements Standards article of this Chapter. A modified system incident audit shall pertain to only the components that were found to compromise the production environment and shall be performed prior to activating the correction in the ERDS for production and operation. This modified system incident audit shall be completed by a DOJ approved Computer Security Auditor 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. A successful modified system incident audit may not replace the biennial audit requirement. A modified system incident audit report shall include, but is not necessarily limited to, all of the following:

(1) Demonstration of the ERDS system in its intended production/operational environment.

(2) The audit shall focus on the cause of the incident of fraud, and show the following:

(A) ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.

(B) Transmissions only occur between authorized parties.

(C) Remnants of sessions, transmissions and ERDS payloads are not stored once the user initiating the session and transmitting ERDS payloads has logged out or been disconnected (either physically or logically).

(D) Authorized and unauthorized users are limited in terms of roles assigned to operate the system.

(E) Auditable events are logged correctly.

(F) Known vulnerabilities have been eliminated or mitigated.

(G) The ERDS is not susceptible to published exploits and that the published updates to the standards and guidelines as described in these regulations shall be implemented within two years.

(H) ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the ERDA.

(I) ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

(3) Documentation must include all of the following:

(A) A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the system.

(B) A review of source code, either selected software components or all software.

(C) An inventory of hardware, software and network devices comprising the system.

(D) An inventory of users and roles authorized to access and operate the system.

(E) A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server, and the ERDS servers visible from a non-ERDS workstation or server.

(F) A review of the ERDS operating procedures established by the County Recorder.

(G) A review of all security checklists established for auditing the ERDS.

(H) A review of contracts with Authorized Submitters.

(I) A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.

(J) A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

(K) That the requirements of these regulations are met.

(4) Upon receipt of the modified system incident audit report, the ERDS Program shall:

(A) Send a written notification within 10 business days to the County Recorder acknowledging receipt of the audit report.

(B) Send a notification of the investigative results and the appropriate action to be taken, if any, to the County Recorder, Board of Supervisors, and District Attorney.

(C) Maintain reports for statistical purposes.

Authority cited: Sections 27393(a), 27393(b) 27393(c), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.

§ 901. Audit Report Format

(a) The format of a security audit report shall include, but is not necessarily limited to, all of the following:

(1) A summary of recommendations in a task-list format.

(2) A description of the DOJ approved Computer Security Auditor’s methodology.

(3) A section for detailed technical observation/recommendation.

(4) A diagram depicting results, where applicable.

(5) Results of testing and reviews.

(6) Recommendations for additional precautions needed to ensure that the system is secure.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.

§ 902. Local Inspection

(a) Counties operating and/or associated with a certified ERDS shall be subject to an ERDS local inspection by an ERDS Program representative in alternating years of the biennial audit. The purpose of this inspection is to ensure that the requirements, as set forth in the regulations, are being adhered to for the ongoing oversight of the ERDS.

(b) An ERDS Program representative shall contact the Lead County Recorder and/or Sub-County Recorder or his or her representative to schedule an on-site inspection of the ERDS and all associated processes on a mutually agreed upon date.

(c) An ERDS Program Policy and Security Review form shall be used to record inspection results. The ERDS Program representative shall verify all of the following:

(1) An auditable log is being maintained for 2 years.

(2) Documentation has been maintained and distributed in cases where an incident has been reported.

(3) Access request and inventory reports are maintained.

(4) The DOJ approved Computer Security Auditor reports are being maintained for a period of 2 years and the following are referenced: ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the ERDA; 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 response to recommendations are being transmitted to the Board of Supervisors, the County Recorder, the County District Attorney and the ERDS Program.

(5) For a Single-County ERDS, that a copy of the following is on file: the County's System Certificate of Operation; the County's Resolution; the County Policy and Procedures; a signed Statement of Understanding form # ERDS 0011; a list of users serving in a role that requires fingerprinting, a signed Acknowledgement of Responsibilities Form # ERDS 0012 for each individual assigned a role that requires fingerprinting; a completed Change of ERDS Role form # ERDS 0008 for individuals that have changed an ERDS role(s) that requires fingerprinting; the DOJ approved Computer Security Auditor ERDS

certificate and contract; the letter of deposit to an approved escrow facility; and the Vendor of ERDS Software certificate and their contract, if any. If internal resources are being used to develop an ERDS in lieu of a vendor, it shall be stated in the county resolution granting establishment of an ERDS.

(6) For a Multi-County ERDS, that a copy of the following is on file: the contract or agreement with other county(s); a list of users, in a role that requires fingerprinting, and classification(s) or employment position(s); a signed Acknowledgement of Responsibilities form # ERDS 0012 for each individual assigned a role that requires fingerprinting; a completed Change of ERDS Role form # ERDS 0008 for individuals that have changed an ERDS role(s) that requires fingerprinting; the Sub-County(ies) resolution; the Application for Sub-County System Certification form # ERDS 0001B; and the Sub-County(ies) Recorder's signed Statement of Understanding form # ERDS 0011.

(d) The ERDS Program representative shall discuss the findings of the inspection with the County Recorder~~,~~ or his or her representative.

(e) A completed Policy and Security Review form shall be signed and dated by both the County Recorder or his or her representative and the ERDS Program representative.

(f) A completed ERDS Program Policy and Security Review form shall be provided to the Lead County Recorder and/or the Sub-County Recorder at the completion of the local inspection. In the case of the Sub-County inspection, a copy of the Policy and Security Review form shall be forwarded to the Lead County.

(g) The ERDS Program representative shall provide an inspection result letter within 10 business days to the County Recorder or his or her representative.

(h) In the case of an inspection resulting in an agency deemed in compliance with all requirements, the ERDS Program representative shall prepare a letter to the County Recorder(s) notifying them of their compliance. In the case of a Multi-County ERDS, the Lead County Recorder shall receive a copy of the Sub-County(ies) letter.

(i) In the case of an inspection resulting in an agency deemed non-compliant with a requirement(s), the ERDS Program representative shall:

(1) Prepare a letter to the County Recorder(s) with notification of the non-compliance. The letter shall contain non-compliance issues requiring corrective action; and a due date shall be assigned allowing 30 days for correction and response. In the case of a Multi-County ERDS, the ERDS Program representative shall forward a copy to the Lead County.

(2) Upon receipt of the County Recorder's response to the request for corrective action, the ERDS Program representative shall review and determine that the non-compliance

issue(s) has been addressed, and shall forward a compliance letter to the County Recorder and/or Sub-County Recorder.

(3) In the case of a response not satisfactorily addressing the non-compliance issues, the ERDS Program representative shall work with the County Recorder and/or Sub-County Recorder to resolve them.

(4) If a response to the corrective action is not received by the due date, the ERDS Program representative shall initiate a follow-up telephone call to inquire on the status of the response. If it is determined that an extension is needed, the County Recorder shall be granted an additional 2 weeks to respond.

(5) If no response is received the ERDS Program representative shall issue a letter of ERDS suspension.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27393(d), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27393(d), 27394, 27396, 27397.5 Government Code.

§ 903. Incident Reporting

(a) A reportable incident of security violation(s) or suspected security violation(s) that compromise the safety or security of an ERDS shall be reported.

(b) The County Recorder shall establish criteria and procedures for handling and responding to incidents.

(c) In the case of a Multi-County ERDS, the Sub-County(ies) shall report security violation(s) or suspected security violation(s) to the Lead County Recorder within 2 business days.

(d) A Fax Transmission Cover Sheet form # ERDS 0007 shall be utilized to notify the ERDS Program of the reportable security violation.

(e) After the fax notification has been made, the County Recorder, either in his or her official capacity or by delegation of the responsibility, shall prepare a detailed incident report that shall include: the date of the incident(s); the parties involved (if known); the nature and scope of the incident(s); and action(s) taken, including steps to protect against future violations.

(f) The detailed incident report shall be forwarded to the ERDS Program, the DOJ approved Computer Security Auditor, District Attorney(s), and their Board of Supervisors within 10 business days of the incident(s) date. The County Recorder shall maintain the report for a period of 2 years and shall be subject to review during local inspections.

(g) Upon receipt of a detailed incident report the ERDS Program shall do the following:

(1) Send a written notification within 2 business days to the reporting party acknowledging receipt of the detailed report.

(2) Send a notification of the ERDS investigative result and the appropriate action to be taken, if any, to the County Recorder, Board of Supervisors, and District Attorney.

(3) Maintain reports for statistical purposes.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.

§ 904. Suspension and Termination of Certification

(a) System certification may be suspended or terminated. All of the following constitute grounds:

(1) Unsatisfactory audit findings by a DOJ approved Computer Security Auditor.

(2) Failure to respond to a notice of corrective action for non-compliance issue(s) as a result of a local inspection.

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

(4) Non-payment of a County's proportionate cost of the System Administration Fee.

(5) A reported security violation that has been determined to compromise the safety or security of an ERDS.

(6) Non-compliance with the Statement of Understanding form.

(7) For good cause.

Authority cited: Sections 27392(a), 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27392(a), 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.

§ 905. Notification

The ERDS Program shall issue a letter of suspension or termination, delivered by certified mail, notifying the County Recorder that the system certification is invalid and shall remain in affect until a reinstatement is granted through the reconsideration process. The County Recorder shall be instructed to immediately cease all operations of the ERDS. A copy of the letter shall be provided to the Board of Supervisors, the Attorney General, and the District Attorney.

Authority cited: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.
Reference: Sections 27393(a), 27393(b), 27393(c), 27394, 27396, 27397.5 Government Code.

§ 906. Reconsideration

(a) A County Recorder may request a reconsideration of a suspension or termination of a system certification. The County Recorder shall submit a written request to the ERDS Program within 30 days of the notification stating justification for the reconsideration. During this time, the County Recorder may not operate the ERDS.

(b) The ERDS Program shall review the request for reconsideration and a determination shall be made in writing to the County Recorder within 30 days.

(c) Reinstatement of an ERDS operation that has been suspended or terminated because of vulnerabilities shall provide a Modified System Incident Audit to the ERDS Program before reinstatement of the ERDS operation. Vulnerabilities include unsatisfactory audit findings by a DOJ approved Computer Security Auditor and/or reported security violations that have been determined to compromise the safety or security of an ERDS.

(d) Reinstatement of an ERDS operation that has been suspended or terminated because of non-compliance to administrative requirements shall be dependant upon responding to and rectifying the reason for suspension or termination. Administrative requirements include failure to respond to a notice of corrective action for a non-compliance issue(s) as a result of local inspection, failure to comply with the audit and local inspection schedule, non-payment of a County's proportionate cost of the System Administration Fee, non-compliance with the Statement of Understanding form # ERDS 0011, and/or good cause.

Authority cited: Sections 27392(a), 27393(a), 27393(b), 27393(c), 27394, 27396, 27397(a), 27397.5 Government Code.
Reference: Sections 27392(a), 27393(a), 27393(b), 27393(c), 27394, 27396, 27397(a), 27397.5 Government Code.