CALIFORNIA DEPARTMENT OF JUSTICE

TEXT OF PROPOSED REGULATIONS

TITLE 11. LAW
DIVISION 1. ATTORNEY GENERAL
CHAPTER 18. ELECTRONIC RECORDING DELIVERY SYSTEM
ARTICLE 2. DEFINITIONS

§ 999.108. Definitions

(a) The following definitions shall apply throughout all the articles within ~~these regulations~~this chapter:

(1) "Agent" means a representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter who ~~has~~is eligible to enter~~ed~~ into a contract with a County Recorder, and, be assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Certified 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~~2) "Attorney General" means the Attorney General of the State of California.

(3) "Availability" means as that term is defined in United States Code, title 44, section 3552, subdivision (b)(3)(C).

~~(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, and, assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.~~

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

(4) "Certified Vendor of ERDS Software" means an entity that sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS. A Certified Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, or County Recorder Designee.

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

(5) "Confidentiality" means as that term is defined in United States Code, title 44, section 3552, subdivision (b)(3)(B).

(~~8~~6) "County Recorder" means a public official responsible for administering an ERDS~~,~~ and ensuring that all ERDS requirements are met, and who oversees the assignment and delegation of ~~the~~ those responsibilities by determining the necessary resources and means.

(~~9~~7) "County Recorder Designee" means a ~~secure access~~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 Computer Security Auditor, Authorized Submitter, Agent, or Certified Vendor of ERDS Software. This role requires fingerprinting.

(~~10~~8) "Developer" ~~has the same meaning as "Vendor".~~means a person or personnel, supporting and/or acting on behalf of the County Recorder and/or Certified Vendor of ERDS Software.

~~(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~~9) "DOJ" means the California Department of Justice.

(~~15~~10) "Electronic Signature of the Notary" means a field, or set of fields, containing information about the electronic signature of the notary who notarized a digital ~~electronic record~~ or digitized ~~electronic~~ record.

(~~16~~11) "ERDA" means the Electronic Recording Delivery Act of 2004, as amended.

(~~17~~12) "ERDS" means an ~~ERDS Program certified~~ Electronic Recording Delivery System certified by the ERDS Program to deliver digitized ~~electronic records~~ and/or digital ~~electronic~~ records to a County Recorder, and, when applicable, return those records to the Agent or Authorized Submitter.

(~~18~~13) "ERDS Account Administrator" means a ~~secure access~~Secure Access role assigned by the County Recorder to an individual who is authorized to configure accounts, assign roles, and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Certified Vendor of ERDS Software. This role requires fingerprinting.

(~~19~~14) "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 Agent or Authorized Submitter via an ERDS.

(~~20~~15) "ERDS Program" means the program within DOJ designated by the Attorney General to certify, implement, regulate, and monitor an ERDS.

(~~21~~16) "ERDS Server" means computer hardware, software, and storage media used by the County Recorder to implement an ERDS. The ERDS Server(s) execute(s) the primary functionality of the application software associated with an ERDS. ~~The ERDS Server includes software for encrypting, decrypting, hashing, submitting, and, when applicable, returning ERDS payloads. It also includes storage media for ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that ERDS server functions can be isolated from other server functions, as evidenced by audit.~~

(~~22~~17) “ERDS System Administrator” means a ~~secure access~~Secure Access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, and network settings, and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Certified Vendor of ERDS Software. This role requires fingerprinting.

(~~23~~18) “FIPS” means Federal Information Processing Standards.

(19) “Hardened” means a security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions or procedures for configuring an IT product to a particular operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product.

(~~24~~20) “HMAC” means Hash Message Authentication Code.

(~~25~~21) “Incident” means an event that may have compromised the ~~safety or~~ security of an ERDS.

(22) “Integrity” means as that term is defined in United States Code, title 44, section 3552, subdivision (b)(3)(A).

~~(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~~23) “Lead County” means the County Recorder in a Multi-County ERDS responsible for administering ~~an~~that ERDS, ensuring that all ERDS requirements are met, and who oversees the assignment and delegation of ~~the~~those responsibilities by determining the necessary resources and means.

(24) A “Licensed and Supported Operating System” means that the operating system is commercially supported and licensed so that security patches and fixes are available.

(~~28~~25) “Live Scan” means a DOJ system used for the electronic submission of applicant fingerprints. ~~This system is outside of the ERDS Program.~~

(~~29~~26) “Logged” means an auditable ERDS event.

(~~30~~27) “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~~28) “MAC” means Message Authentication Codes.

(~~32~~29) “Multi-County” means an ERDS application ~~where~~in which County Recorders collaborate and make use of a single ERDS serving multiple counties.

(~~33~~30) “NIST” means National Institute of Standards and Technology.

(~~3430~~31) “Non-Substantive Modification” means a change that does not affect the functionality of an ERDS.

~~(35) “ORI” means Originating Agency Identifier.~~

(~~36~~32) “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~~33) “Public Entity” includes the ~~State~~state, the Regents of the University of California, the Trustees of the California State University and the California State University, a county, city, district, public authority, public agency, and any other political subdivision or public corporation in the ~~State~~state. As provided in this chapter, “public entity” also includes federal government entities.

~~(38) “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.~~

(~~39~~34) “Reportable” means an incident that has ~~resulted in the compromise of~~compromised the ~~safety or~~ security of an ERDS and shall be reported to the ERDS Program.

~~(40) “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.~~

(~~41~~35) “Role” means a security mechanism, method, process, or procedure that defines specific privileges dictating the level of access to an ERDS.

(~~42~~36) “Secure Access” means a role assigned by the County Recorder to an individual which requires fingerprinting ~~to~~and includes: 1) ~~An~~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~~a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) ~~An~~an ERDS System Administrator who is authorized to configure hardware, software and network settings; 4) ~~An~~an ERDS Account Administrator who is authorized to configure accounts, assign roles, and issue credentials; 5) ~~An~~an individual who is granted ~~physical access~~Physical Access to an ERDS server; 6) ~~A~~a County Recorder Designee authorized to retrieve, and, when applicable, return ~~of~~ submitted ERDS payloads; 7) Certified Vendor of ERDS Software personnel who support or act on behalf of the Certified Vendor of ERDS Software; or 8) a Developer acting in lieu of a Certified Vendor of ERDS Software.

~~(43) “Security Testing” means an independent security audit by a Computer Security Auditor, including, but not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.~~

~~(44) “SHA” means Secure Hash Algorithm.~~

~~(45) “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.~~

(37) “Single-County” means an ERDS application in which a County Recorder’s Office connects to the ERDS system individually.

(~~46~~38) “Source Code Materials” ~~means~~includes, but is not limited to, all of the following: 1) ~~A~~a copy of all source code that implements ERDS functionality; 2) ~~A~~a copy of the compiler needed to compile the ERDS source code in escrow; 3) ~~Instructions~~instructions for installation and use of the ERDS source code compiler; and 4) ~~Instructions~~instructions that facilitate reviews, modification, and/or recompiling the source code.

(~~47~~39) “Sub-County” means ~~the collaborating~~a County Recorder(s) of a county other than the Lead County in a Multi-County ERDS ~~operation~~.

(~~48~~40) “Substantive Modification” means a change that affects the functionality of an ERDS.

~~(49) “TLS” means Transport Layer Security.~~

(~~50~~41) “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.~~

(~~51~~42) “User” means a person who uses a computer to access, submit, retrieve, or, when applicable, return an ERDS payload.

~~(52) “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 counties for establishing an ERDS. A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, or County Recorder Designee or internal county resources used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.~~

(~~53~~43) “Workstation” means a computer used to connect to, and/or interact with, an ERDS.

Authority cited: Section 27393, Government Code.
Reference: Sections 27390(b), 27393(b)(4), 27395(f), 811.2, 15000, and 12510, Government Code.

§ 999.122. Role-Based Fingerprinting Requirement.

(a) The following ERDS roles assigned ~~secure access~~Secure Access ~~to both Type 1 and 2 instruments, (excludes Type 2 instruments only),~~ require the submission of fingerprints to the DOJ, and require clearance based on the state and federal criminal record checks, prior to the individual serving in the role as an/a:

(1) Authorized Submitter or Agent ~~or representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter.~~ that has entered into a contract with a County Recorder and submits directly to an ERDS.

~~(2) Authorized Submitter and his/her employees is a party that has entered into a contract with a County Recorder.~~

(~~3~~2) Computer Security Auditor.

(4~~3~~) County Recorder Designee.

(~~5~~4) ERDS Account Administrator.

(~~6~~5) ERDS System Administrator.

(~~7~~6) An individual who is ~~authorized~~granted ~~physical~~Physical ~~access~~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~~7) Certified Vendor of ERDS Software ~~(or Developer)~~ personnel~~,~~ who support~~ing~~ and/or act~~ing~~ on behalf of the ~~certified~~Certified Vendor of ERDS Software.

(~~9~~8) ~~Internal county resources used as a~~Developer ~~of ERDS in lieu of a Vendor of ERDS Software~~.

Authority Cited: Sections 27393, 27395(~~d~~a), and 27395(~~e~~b), Government Code.
Reference: Sections 27393(b)(9)~~,~~ and 27395, Government Code.

§ 999.128. Basis for the Baseline Requirements and Technology Standards.

(a) To meet the intent of the ERDA, the minimum standards and guidelines established within ~~these regulations~~this chapter are based on information security "best practices" designed to offer a layered security approach through the use of the following security objectives: Confidentiality, Integrity, and Availability.

~~(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 procesess. Confidential protection applies to data in storage, during processing, and while in transit.~~

Note: Authority cited: Section 27393, Government Code. Reference: Section 27393(b), Government Code.

§ 999.129. Standards and Guidelines.

Standards and guidelines contained in ~~these regulations~~this chapter are based on ~~National Institute of Standards and Technology (~~NIST~~)~~ and ~~Federal Information Processing Standard (~~FIPS~~)~~ publications, including: NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization (publication date, ~~September 2006~~December 2014); FIPS 180-4, Secure Hash Standard (SHS) (publication date, ~~March 2012~~August 2015); FIPS 140-2, Security Requirements for Cryptographic Modules (publication date, May 2001, as amended by change notice issued~~with a change notice dated~~, December 2002); FIPS 197, Advanced Encryption Standard (AES) (publication date, November 2001); FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC) (publication date, July 2008); NIST Special Publication ~~800-63-2, Electronic Authentication Guideline~~800-63-3, Digital Identity Guidelines (publication date, ~~August 2013~~June 2017); NIST Special Publication 800-70 Revision ~~2~~4, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date, ~~February 2011~~February 2018); FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013); NIST Special Publication 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (publication date, April 2014); FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (publication date, August 2015). The ERDS Program shall make available any update, revision, or replacement of a ~~reference cited~~standard or guideline cited in this provision.

Note: Authority cited: Section 27393, Government Code. Reference: Section 27393(b), Government Code.

~~§ 999.130. Instrument Type.~~

~~(a) The ERDA refers to two types of instruments that may be delivered, and, when applicable, 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.~~

~~Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27397.5(a) and 27397.5(a), Government Code.~~

§ 999.131. 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 ~~these regulations~~this chapter.

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

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

§ 999.132. 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.", ~~and identified as a Type 1 or Type 2 or Type 1 and 2, and return, when applicable.~~ 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~~Confidentiality and ~~integrity~~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~~this chapter.

Note: Authority cited: Sections 27392(a) and 27393, Government Code. Reference: Sections 27392(a), 27393, 27396(a), and 27397.5(a), Government Code.

§ 999.133. Payload Structure, Content and Usage.

(a) All ERDS ~~for either Type 1 or Type 2 instruments~~ shall contain a~~n ERDS~~ a 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~~b) 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.~~

(ec) Multiple digital ~~electronic records~~ or digitized ~~electronic~~ records within the same payload are allowed~~; only Secure Access users are authorized to include both Type 1 and Type 2 instruments in the same ERDS payload~~.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27391(e), 27392(b), and 27393(b)(10), Government Code.

§ 999.134. Uniform Index Information.

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

Note: Authority cited: Section 27393, Government Code. Reference: Section 27393(b)(10), Government Code.

~~§ 999.135. 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.~~

~~Note: Authority cited: Section 27393, Government Code. Reference: Section 27391(e), Government Code.~~

§ 999.136. 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~~:~~ malware (such as viruses,

worms, Trojan Horses, spyware, or adware) and executable software~~,~~ (such as ActiveX components, ~~java script~~JavaScript, ~~java~~Java components, or HTML-encoded hyperlinks~~), and any other executable software~~.

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

(c) All ERDS shall use hashing to protect the Integrity of ERDS payloads. Hashing message digest size shall be a minimum of 224 bits. Hashing shall comply with FIPS 180-4, Secure Hash Standard (SHS) (publication date, August 2015) or FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (publication date, August 2015).

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), and 27397.5(a), Government Code.

§ 999.137. ~~Security~~ Encryption Requirements ~~for Payload Protection~~.

(a) ~~For a~~All ERDS~~, either Type 1 or Type 2 instruments~~ shall employ encryption, both in transmission and ~~storage~~at-rest, 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:~~

(b) Encryption shall be a minimum of 128 bit.

(c) When encryption is employed, the cryptographic modules shall be certified to meet FIPS 140-2, Security Requirements for Cryptographic Modules (publication date May 2001, as amended by change notice issued December 2002).

~~(1) The Algorithm developed by Rivest, Sharmin and Adleman (RSA) specified in ANS x9.31 and PKCS #1 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 2001).~~

~~(b) For all ERDS, either Type 1 or Type 2 instruments shall use hashing to protect the integrity of ERDS payloads. For all ERDS certified before January 1, 2015, the approved hash function for ERDS payloads is the Secure Hash Algorithm as defined in FIPS 180-2, Secure Hash Standard (publication date August 2002 with change notice dated February 2004), using a message digest size of at least 224 bits until January 1, 2016. After January 1, 2016, all ERDS certified before January 1, 2015 shall comply with FIPS 180-4, Secure Hash Standard (publication date, March 2012). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. All ERDS certified after January 1, 2015 shall comply with FIPS 180-4, Secure Hash Standard (publication date, March 2012).~~

~~(c) For all ERDS either Type 1 or Type 2 instruments shall use Digital Signatures to assure the authenticity of ERDS payloads. For all ERDS certified before January 1, 2015, the approved signing function approved for ERDS payloads is the RSA algorithm, using a minimum key-length of 1024 bits until January 1, 2016. After January 1, 2016, all ERDS certified before January 1, 2015 shall comply with the digital signature algorithms approved as defined in FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. All ERDS certified after January 1, 2015 shall comply with the digital signature algorithms approved as defined in FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013).~~

~~(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 2001 with a change notice dated December 2002).~~

~~(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 instruments: 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.~~

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b) and 27397.5, Government Code.

§ 999.138. 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~~Hardened following NIST Special Publication 800-70 Revision 4, National Checklist for IT Products-Guidelines for Checklist Users and Developers (publication date, February 2018). As such, workstations used to submit, retrieve, or, when applicable, return 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) A Licensed and Supported Operating S~~s~~ystem and application software with the most up-to-date patches and hot-fixes.

(3) ~~Host based firewall configured to restrict inbound and outbound connections~~Validated system configuration in accordance with operating system, application, and firewall checklists available in the National Checklist Program (NCP) repository. Checklists published by the following government and private entities shall be used before any other: United States Government Configuration Baseline (USGCB), Defense Information Systems Agency (DISA), United States Department of Defense (DOD), National Security Agency (NSA), Center for Internet Security (CIS), and The MITRE Corporation. All non-compliance shall be documented in a manner that states the reason for non-compliance and a plan of action to obtain compliance, mitigation, or acceptance of the risk by the applicable counties.

(b) ~~For Type 1 instruments only, i~~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 ~~provisions~~subdivisions (a) and (b) as ~~a~~ mandatory requirements in all contracts with Authorized Submitters. An Authorized Submitter must~~whom shall~~ ensure that an Agent, if any, complies with ~~these regulations~~the provisions of this chapter. The contents of these contract provisions are subject to audit and local inspection.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.139. 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~~a) Fixed and removable disks ~~for either Type 1 or Type 2 instruments~~ shall be sanitized as defined in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization (publication date, ~~September 2006~~December 2014), prior to reallocating ERDS hardware or storage media to other purposes.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), and 27397.5, Government Code.

§ 999.140. ERDS Identification Security Requirements.

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

(1) User accounts ~~may~~shall be implemented as part of an ~~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~~account shall be uniquely identified and individually assigned.

(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~~C) User accounts shall be associated with ERDS roles.

Note: Authority cited: Section 27393(b), Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.141. ERDS Authentication Security Requirements.

(a) ERDS ~~that serve Type 1 and 2 instruments shall be required to meet all of the additional~~ authentication security requirements shall meet Authenticator Assurance Level (AAL) 2 or higher as defined by NIST Special Publication 800-63-3, Digital Identity Guidelines (publication date, June 2017).~~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) For all ERDS certified before January 1, 2015, authentication assurance shall meet Level 3 or higher, as defined by the NIST Special Publication 800-63, Electronic Authentication Guideline (publication date April 2006 Version 1.0.2) until January 1, 2016. After January 1, 2016, all ERDS certified before January 1, 2015 shall meet authentication assurance Level 3 or higher, as defined by NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. All ERDS certified after January 1, 2015 shall meet authentication assurance Level 3 or higher, as defined by NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013).~~

~~(3) For all ERDS certified before January 1, 2015, 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, Electronic Authentication Guideline (publication date April 2006 Version 1.0.2), is achieved until January 1, 2016. After January 1, 2016, for all ERDS certified before January 1, 2015, 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 800-63-2, Electronic Authentication Guideline (publication date, August 2013) is achieved. Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. For all ERDS certified after January 1, 2015, 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 800-63-2, Electronic Authentication Guideline (publication date, August 2013) is achieved.~~

~~(b) Password creation, protection, maintenance, processing and handling shall adhere to the Password Policy contained in the California Counties Best Practices Information Security Program (publication date March 2002).~~

Note: Authority cited: Section 27393(b), Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.142. ERDS Role-Based Security Requirements.

(a) All ERDS ~~that serve either Type 1 or Type 2 instruments~~ shall be required to meet all of the role-based security requirements 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~~Which ERDS payloads will be displayed.

(C) Whether or not ERDS payloads may be submitted, retrieved, and, when applicable, 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~~3) ~~If~~Upon notification of a user's status change~~s~~ so that access to ERDS is no longer required, the user's ERDS account and identity credentials shall be disabled and revoked by the County Recorder within 30 days from the date of the notice or subject to the terms of the County Recorder's documented procedure on how to decommission users~~for the purposes of ERDS~~. ~~ERDS user accounts and identity credentials may not be transferable.~~

(4) ERDS user accounts and identity credentials are not transferable.

(5) Identity credentials shall be recognized across a Multi-County 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, t~~The agreement shall be made part of the ERDS operating procedures of all County Recorders who are ~~party~~parties 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, and, when applicable, returned.

(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~~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 and Agent, if any, shall be limited to those privileges granted by the County Recorder. The Authorized Submitter and Agent are prohibited from submitting ERDS payloads on behalf of another Authorized Submitter, or Agent, ~~unless the details of the agreement are specified~~except as authorized by contract ~~in contracts~~ with the County Recorder. ~~Regardless of the details of the agreement, s~~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 being represented in ~~a~~each transaction.

(10) An Authorized Submitter who has no access to an ERDS and submits through an Agent is not subject to the requirements of Government Code Section 27395.

(11) An Authorized Submitter pursuant to Government Code Section 27391(c)(1) who has no access to an ERDS and submits through an Agent is subject to the requirements of Government Code Section 27391(c)(2).

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27390(b)(1), 27391, ~~and~~ 27393(b)(2), and 27395, Government Code.

§ 999.143. ERDS Server Security Requirements.

(a) An ERDS that employs one or more servers ~~that serve Type 1 or Type 1 and 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 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) Proxy servers may not execute an ERDS functionality except as described above.~~

~~(5) The ERDS server shall communicate via secure sessions through the proxy server when interoperating via the Internet. As a minimum, sessions between the proxy server and the 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 application software, store ERDS payloads, authenticate ERDS credentials, control ERDS access based on assigned roles, and log ERDS transactions.~~

(~~7~~2) ERDS servers shall be configured to prevent unauthorized access, modification, or use.

(~~8~~3) 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 an ERDS are Hardened according to one of the following checklists or guidelines:

(A) ~~For all County Recorder ERDS certified before January 1, 2015, NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products (publication date, May 2005) until January 1, 2016. After January 1, 2016, f~~For all ERDS certified before January 1, ~~2015~~2019, NIST Special Publication 800-70 Revision ~~2~~4, ~~Security Configuration Checklists~~National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date, February 2011), until January 1, 2020. After January 1, 2020, for all ERDS certified before January 1, 2019, NIST Special Publication 800-70 Revision 4, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers

(publication date, February 2018). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. For all ERDS certified after January 1, ~~2015~~2019, NIST Special Publication 800-70 Revision ~~2~~4, ~~Security Configuration Checklists~~National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date, ~~February 2011~~February 2018).

(B) ~~Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.~~Checklists published by the following government and private entities shall be used before any other: United States Government Configuration Baseline (USGCB), Defense Information Systems Agency (DISA), United States Department of Defense (DOD), National Security Agency (NSA), Center for Internet Security (CIS), and The MITRE Corporation. All non-compliance shall be documented in a manner that states the reason for non-compliance and a plan of action to obtain compliance, mitigation, or acceptance of the risk by the applicable counties.

(~~9~~4) All county servers used for an ERDS shall have a ~~host-based~~ file integrity checking system ~~configured to alert the ERDS System Administrator of an operating system file change to the ERDS server and have anti-malware software installed and operating to protect the server~~.

(5) All county servers used for an ERDS shall be configured to alert the ERDS System Administrator of an operating system file change to the ERDS server.

(6) All county servers used for an ERDS shall have anti-malware software installed that operates upon boot-up.

(7) Digitized electronic records submitted to an ERDS must be scanned by anti-malware software.

(8) All inputed fields shall have input validation.

(9) All county servers used for an ERDS shall have a Licensed and Supported Operating System and application software with the most up-to-date patches and hot-fixes.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.144. ERDS Security Requirements for Network Security.

(a) An ERDS ~~that serve Type 1 or Type 1 and 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)~~(1) ERDS shall comply with the minimum requirements set forth in NIST Special Publication 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (publication date, April 2014).~~For all ERDS certified before January 1, 2015, the standard for establishing secure connection is the Transport Layer Security (TLS) protocol 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, "Advanced Encryption Standard", (publication date, November 2001) until January 1, 2016. After January 1, 2016, for all ERDS certified before January 1, 2015, the standard for establishing secure connection is the TLS protocol described in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013). As a minimum,128-bit encryption shall be used to establish secure TLS sessions, as described in FIPS 197, "Advanced Encryption Standard," (publication date, November 2001). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. For all ERDS certified after January 1, 2015, the standard for establishing secure connection is the TLS protocol described in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013). As a minimum, 128-bit encryption shall be used to establish secure TLS sessions, as described in FIPS 197, "Advanced Encryption Standard," (publication date, November 2001).~~

~~(4) ERDS shall employ Message Authentication Code (MAC) to assure the authentication of encrypted ERDS payloads. For all ERDS certified before January 1, 2015, MACs shall conform to the standard defined in FIPS 198, "The Keyed-Hash Message Authentication Code (HMAC)", (publication date March 2002) until January 1, 2016. After January 1, 2016, for all ERDS certified before January 1, 2015, MACs shall conform to the standard defined in FIPS 198-1, "The Keyed-Hash Message Authentication Code (HMAC)", (publication date, July 2008). Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. For all ERDS certified after January 1, 2015, MACs shall conform to the standard defined in FIPS 198-1, "The Keyed-Hash Message Authentication Code (HMAC)", (publication date, July 2008).~~

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

~~(6)~~(2) Network security controls shall be implemented to prevent unauthorized network traffic from reaching ERDS components.

~~(7)~~(3) 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~~ securely in the event of an operational failure.

(D) ~~Detect possible intrusions and, if a possible intrusion is detected, alert the ERDS System Administrator and take action to prevent the intrusion.~~An intrusion detection and prevention technology shall be configured to alert and or prevent intrusion into the ERDS.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.145. 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~~that prevents unauthorized physical access.

(b) All ERDS ~~that serve either Type 1 or Type 2 instruments~~ shall be required to meet all of the physical security requirements as follows:

(1) 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 the County Recorder ERDS operating procedures or may be established by mutual agreement between the County Recorder and the entity housing the ERDS server.

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

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

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

(1) Persons who are ~~authorized physical access~~granted Physical Access to an ERDS server require fingerprinting.

(2) All requests for ~~physical~~Physical ~~access~~Access to a~~n~~ single-purpose ERDS server are subject to ~~dis~~approval by the County Recorder. Absent an agreement to the contrary, the County recorder cannot grant Physical Access to a multi-purpose server for non-ERDS purposes. ~~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.~~

(3) The County Recorder will account~~An inventory that accounts~~ for all keys, whether physical or electronic, used for locking and unlocking ~~physical~~Physical ~~access~~Access to an ERDS server, software, and/or data ~~shall be completed at least every 90 calendar days~~using a process determined by the County Recorder and contained in the ERDS Operating Procedures.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27393(c), and 27397.5, Government Code.

§ 999.146. 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 or manual processes. Logs shall be safely stored and maintained in a manner that ensures their availability for (1) a period of at least twenty-four (24) months, or (2) at least one (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~~this chapter.

(c) Incident reporting shall comply with provisions contained within ~~these regulations~~this chapter.

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

(1) ~~For Type 1 only, l~~Login successes and failures.

(2) ~~For Type 1 only, s~~Session starts and ends.

(3) ~~For Type 1 only, s~~Session timeouts.

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

(5) ~~For Type 1 only,~~ ERDS transactions 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~~.

(6) ~~For Type 1 only,~~ ERDS sessions ~~is~~ terminated within a preset timeout limit without receiving a logout command.

(7) ~~For Type 1 only, u~~Unauthorized access attempts, including, but not limited to~~:~~ unauthorized users attempting either physical or logical access~~, either physical or logical,~~ to ERDS storage areas. This is an ~~incident~~Incident and shall be reported if fraud is suspected.

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

(9) ~~For Type 1 only, p~~Privilege elevation. This is an ~~incident~~Incident and shall be reported.

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

(11) Authentication failures.

(12) ERDS accounts locked out and/or disabled due to failed consecutive login attempts. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(13) Auditable events that overwrite other logged events. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(14) Auditable events that cannot be logged. This is an ~~incident~~Incident.

~~(15) Logs consume 95% or more of the storage space allocated for logging. This is an incident.~~

(~~16~~15) Logs that cannot be safely stored. This is an ~~i~~Incident

(~~17~~16) ~~For Type 1 only,~~ ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not. This is an ~~incident~~Incident only if not authorized and shall be reported if fraud is suspected.

(~~18~~17) ~~For Type 1 only, h~~Hardware or software configuration changes. This is an ~~incident~~Incident only if not authorized and shall be reported.

~~(19) Unique name of the ERDS payload. This is an incident only if out of sequence.~~

(~~20~~18) Dates and times the ERDS payload was submitted, retrieved or, when applicable, returned. This is an ~~incident~~Incident only if the dates and times are not current.

(~~21~~19) Identity of ~~the~~an individual, who submitted, retrieved, or, when applicable, returned ~~the~~an ERDS payload. This is an ~~incident~~Incident only if ~~not authorized,~~the individual is not authorized for Secure Access to the ERDS.

(~~22~~20) Name of the organization that ~~the~~an individual represented while submitting, retrieving or, when applicable, returning ~~the~~an ERDS payload. This is an ~~incident~~Incident only if ~~not authorized.~~the individual is not authorized for Secure Access to the ERDS.

(~~23~~21) ~~For Type 1 only, a~~A transmission failure.

(~~24~~22) ~~For Type 1 only, a~~A storage failure.

(~~25~~23) A decryption failure. This is an ~~incident~~Incident and shall be reported if fraud is suspected.

(~~26~~24) A hash failure. This is an ~~incident~~Incident and shall be reported if fraud is suspected.

(~~27~~25) A validity check failure. This is an ~~incident~~Incident and shall be reported if fraud is suspected.

(~~28~~26) ~~Type 1 or Type 2 i~~An instrument submitted unencrypted. This is an ~~incident~~Incident and shall be reported.

~~(29) Type 1 instrument submitted as a Type 2 instrument or vice versa. This is an incident and shall be reported if fraud is suspected.~~

~~(30) Type 1 instrument submitted via an Authorized Access ERDS. This is an incident and shall be reported if fraud is suspected.~~

(~~31~~27) Unauthorized components that draw data or images from sources external to the digital ~~electronic record~~ or digitized ~~electronic~~ record. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(~~32~~28) Unauthorized transactions submitted via an ERDS~~, including but not limited to, instruments that are neither Type 1 nor Type 2~~. This is an ~~i~~Incident and shall be reported if fraud is suspected.

(~~33~~29) ~~For Type 1 only, s~~Server failures, including, but not limited to, hardware, software, and network component failures, that causes the ERDS to be unavailable or that exposes the ERDS

server directly to the Internet. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(~~34~~30) Events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(~~35~~31) ~~For Type 1 only, u~~Unauthorized changes to the ERDS operational configuration. This is an ~~incident~~Incident and shall be reported if fraud or intrusion is suspected.

(~~36~~32) ~~For Type 1 only, n~~Network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(~~37~~33) ~~For Type 1 only, e~~Events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an ~~incident~~Incident and shall be reported if intrusion is suspected.

(~~38~~34) Inability to obtain and employ up-to-date anti-malware software.

(~~39~~35) Inability to obtain and employ cryptography, including hashing, encryption, and decryption. This is an ~~incident~~Incident and shall be reported.

(~~40~~36) Inability to obtain and employ the most up-to-date patches and hot-fixes.

(~~41~~37) Unauthorized access or changes to storage media~~,~~ and improper sanitization of storage media. This is an ~~incident~~Incident and shall be reported if compromise of the storage media is suspected.

(~~42~~38) Any other event that compromises the ~~safety or~~ security of ~~an~~the ERDS. This is an ~~incident~~Incident and shall be reported.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), 27394, and 27396, Government Code.

§ 999.147. Proprietary Software.

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

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

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

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

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

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

Note: Authority cited: Sections 27393, 27394(e), and 27394(f), Government Code. Reference: Sections 27393(b)(2), 27393(b)(11), and 27394(e), Government Code.

§ 999.148. Escrow Requirements.

(a) ERDS source code materials shall be placed into an ~~approved~~ escrow facility approved by the County Recorder when an ERDS is developed for a County Recorder. For each submission, the materials placed in escrow shall be sufficient to maintain the 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~~b) 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~~including~~the~~ tools and documentation, ~~to allow~~that allows 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.

Note: Authority cited: Sections 27393 and 27394(e), Government Code. Reference: Sections 27393(b)(5) and 27394(e), Government Code.

§ 999.149. 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.~~

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27393(b)(5), and 27393(c), Government Code.

§ 999.150. 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 Certified Vendor of ERDS Software and/or Developer~~of ERDS Software~~ 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) That the escrow company, its officers, and directors~~,~~ may not hold or exercise a direct or indirect financial interest~~(s)~~ in the Certified Vendor of ERDS Software or the County Recorder.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27393(b)(5), and 27393(c), Government Code.

~~§ 999.153. Access to Materials.~~

~~Escrow agreements shall allow for access to ERDS source code materials by a Computer Security Auditor hired for the purpose of conducting computer security audits.~~

~~Note: Authority cited: Sections 27393 and 27394(e), Government Code. Reference: Sections 27393(b)(5), 27393(c) and 27394(e), Government Code.~~

§ 999.154. Escrow Agreement State Non-Responsibility.

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

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

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(a), 27393(b), 27393(b)(5), 27393(c), 27394(a), and 27397, Government Code.

§ 999.165. 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 these regulations~~.

(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 and/or Agents who~~m shall ensure that an Agent, if any, complies with these regulations~~ have Secure Access to that ERDS.

(e) Prior to entering into a contract with an Authorized Submitter described in Government Code section 27391(c)(1), a County Recorder shall require the Authorized Submitter and any Agent submitting documents on behalf of the Authorized Submitter to provide proof of financial responsibility in the form of a certificate of insurance evidencing one million dollars ($1,000,000) of general liability coverage.

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

~~(f)~~(g) A County Recorder shall enter into a contract with a Computer Security Auditor, who has a valid Computer Security Auditor Certificate issued by the ERDS Program, for the purpose of meeting the audit and oversight requirements as ~~contained within these regulations~~set forth in this chapter.

~~(g)~~(h) A County Recorder shall be required to verify, prior to entering into a contract with a Certified Vendor of ERDS Software, if any, that the ~~Vendor~~vendor has a valid Certified Vendor of ERDS Software Certificate issued by the ERDS Program.

~~(h)~~(i) The County Recorder shall be responsible for administering an ERDS~~,~~ and establishing and following ERDS policies and procedures that include all of the following requirements:

(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 all individuals designated as having ~~secure~~Secure ~~access~~Access ~~and/or authorized access~~ to operate the ERDS ~~and informing the ERDS Program of role changes for those individuals requiring fingerprinting by submitting the Change of ERDS Role form # ERDS 0008 (May 2011) to the ERDS Program~~. A copy of the list of all users with ~~secure~~Secure ~~access~~Access ~~and/or authorized access is to~~shall be maintained for review during audits and local inspections.

(3) Ensure users with roles authorized to access and operate the ERDS understand and sign the Acknowledgement of Responsibilities form # ERDS 0012 (May 2011) and that a copy is maintained for review during audits and local inspections.

(4) ~~The County Recorder shall establish~~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 ~~these regulations~~this chapter.

Note: Authority cited: Sections 27393, 27394(a), and 27394(c), Government Code. Reference: Sections 27391, 27392(a), 27393, 27394(a), 27394(c), 27394(f), and 27397.5, Government Code

§ 999.166. 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) A County Recorder may apply for the initial certification of an ERDS as either a Single-County or Multi-County ERDS ~~and shall designate as either a Type 1 or Type 2 or a Type 1 and 2 operation,~~ and, when applicable, return function via an ERDS. ~~An ERDS may not be implemented prior to receipt of ERDS Program's approval of the application.~~

(~~c~~b) An ERDS may not be implemented prior to receiving a System Certificate of Operation from the ERDS Program.

(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~~submit to the ERDS Program all of the following:

(A) ~~Submit an~~An Application for System Certification form # ERDS 0001A (May 2011) to the ERDS Program, which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(B) ~~Submit a~~A copy of the ~~County Resolution~~resolution to establish an ERDS as approved by ~~the Board of Supervisors~~its county board of supervisors. The resolution shall include, but not be limited to~~, instrument type~~, designating the ERDS as Single-County~~,~~ or Multi-County, and, when applicable, the return function via an ERDS.

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

(D) ~~Submit a~~A copy of the Certified Vendor of ERDS Software contract, if any. If internal county resources and/or another public entity are being used to develop an ERDS in lieu of a Certified Vendor of ERDS Software, ~~it~~that shall be stated in the ~~County~~ county ~~Resolution~~resolution ~~granting~~approving establishment of ~~an~~the ERDS.

(E) ~~Submit a~~A copy of ~~the County's~~its contract with a Computer Security Auditor.

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

(G) ~~Submit p~~Proof of fingerprint submission for individuals designated as having a role that requires fingerprinting and a copy of the list of all users with ~~secure and/or authorized access~~Secure Access.

(H) ~~Submit a~~A signed and dated Statement of Understanding form # ERDS 0011 (May 2011) declaring under penalty of perjury under the laws of the State of California that all information contained therein 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~~submit to the ERDS Program all of the following:

(A) ~~Submit a~~An Application for System Certification form # ERDS 0001A (May 2011) to the ERDS Program, which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(B) ~~Submit the~~A copy of the ~~Lead County's R~~resolution to establish a Multi-County ERDS as approved by the Lead County~~Board of Supervisors~~ board of supervisors.

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

(D) ~~Submit a~~A copy of the Certified Vendor of ERDS Software contract, if any. If internal county resources and/or another public entity are being used to develop an ERDS in lieu of a Certified Vendor of ERDS Software, that~~it~~ shall be stated in the ~~County~~county ~~Resolution~~resolution ~~granting~~approving the establishment of the~~an~~ ERDS.

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

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

(G) ~~Submit p~~Proof of fingerprint submission for individuals designated as having a role that requires fingerprinting and a copy of the list of all users with ~~secure and/or authorized access~~Secure Access.

(H) ~~Submit all~~The documentation for each Sub-County~~(ies) documentation~~ that will participate in the ERDS listed in subdivision (b)(3) of this section as an attachment to the Application for System Certification form # ERDS 0001A~~application~~.

(I) ~~Submit a~~A signed and dated Statement of Understanding form # ERDS 0011 (May 2011) declaring under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(3) ~~A County Recorder applying as a~~A Sub-County ~~during the~~that will participate ~~initial certification of a Multi-County ERDS shall comply with all of the following~~ in a Multi-County ERDS for which initial certification is sought shall provide all of the following to the Lead County:

(A) ~~Submit a~~An Application for Sub-County System Certification form # ERDS 0001B (May 2011) to the Lead County, which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(B) ~~Submit a~~A copy of the ~~Sub-County's R~~resolution to participate in a Multi-County ERDS as approved by the Sub-County board of supervisors~~Board of Supervisors~~.

(C) ~~Submit p~~Proof of fingerprint submission for individuals designated as having a role that requires fingerprinting and a copy of the list of all users with ~~secure and/or authorized access~~Secure Access.

(D) ~~Submit a~~A signed and dated Statement of Understanding form # ERDS 0011 (May 2011) declaring under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

Note: Authority cited: Sections 27393, 27394(a), and 27395(b), Government Code. Reference: Sections 27390(b)(8), 27391(a), 27392, 27393(b)(2), 27394(a), and 27395(b), Government Code.

§ 999.167. Substantive Modification(s).

A substantive modification occurs when a change affects the functionality of an ERDS. Substantive modifications include, but are not limited to, any of the following:

(1) Changes to source code that lead to new or different functional behaviors; ~~or~~

(2) Changes to call signatures in source code interfaces to purchased components; ~~or~~

(3) Changes of data structures or structural database objects; ~~or~~

(4) Changes that require modification of deployment procedures; ~~or~~

(5) A new version of a compiler that requires source code changes in order to compile existing source code error and warning free; ~~or~~

(6) Changes to purchased components or components that are part of software libraries; ~~or~~

(7) Relocation of an ERDS server to a different network segment; ~~or~~

(8) Changing an ERDS server from ~~a~~ single-purpose to multi-purpose; ~~or~~

(9) Changing an ERDS server from ~~a~~ Single-County to a Multi-County; ~~or~~

(10) Hardware maintenance involving the complete replacement of an ERDS; ~~or~~

(11) Software maintenance releases that correct, perfect, enhance, or otherwise affect the functionality of ERDS; or

~~(12) When changing an instrument Type; or~~

(~~13~~12) Changing to a return capability.

Note: Authority cited: Sections 27393, 27394(a), and 27395(b), Government Code. Reference: Sections 27393(b)(2) and 27393(b)(6), Government Code.

§ 999.168. Substantive Modification~~(s)~~ Application Procedure.

(a) Following initial system certification, ~~a Request for Approval of Substantive Modification(s) form # ERDS 0013 (May 2011), as defined within these regulations~~approval by the ERDS program of any Substantive Modification~~,~~ 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. A brief description of the change of the functionality shall be included on the Request for Approval of Substantive Modification(s) form # ERDS 0013 (May 2011)~~. ThisThe modified system audit shall be completed by a 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 fifteen (15) business days of the provisional implementation, the County Recorder shall apply for approval of the substantive modification(s) in order for the ERDS Program to make a final approval determination status.

(b) ~~Requests for approval of substantive modification(s) shall be submitted to the ERDS Program as follows~~A County Recorder applying for approval of a Substantive Modification other than adding a Sub-County to a Multi-County ERDS shall submit to the ERDS Program all of the following:

(1) ~~Submit a~~A Request for Approval of Substantive Modification(s) form # ERDS 0013 (May 2011), which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information is true and correct.

(2) If using a Certified Vendor of ERDS Software and/or Developer, ~~S~~ssubmit a copy of the proof of escrow letter of deposit.

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

(4) ~~Submit a~~A copy of the County's contract with a Computer Security Auditor.

(5) ~~Submit a~~A copy of the ~~successful Modified System Audit Report~~report for the modified system audit report ~~conducted by a Computer Security Auditor~~required by subdivision (a) of this section.

(c) ~~Requests for approval of substantive modification(s) for adding a Sub-County, the Lead County shall submit to the ERDS Program as follows~~A County Recorder applying for approval of a Substantive Modification to add a Sub-County to a Multi-County ERDS shall submit to the ERDS Program all of the following:

(1) ~~Submit a~~A Request for Approval of Substantive Modification(s) form # ERDS 0013 (May 2011), which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(2) A copy of the resolution to participate in the Multi-County ERDS as approved by the ~~Board of Supervisors~~Sub-County board of supervisors.

(3) ~~Submit a~~A copy of the proof of escrow letter of deposit.

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

(5) ~~Submit a~~A copy of the County's contract with a Computer Security Auditor.

(6) ~~Submit a~~A copy of the ~~successful Modified System Audit Report conducted by a Computer Security Auditor~~report for the modified system audit report required by subdivision (a) of this section.

(7) ~~Submit the Sub-County's Application for Sub-County System Certification form # ERDS 0001B (May 2011) and required documentation as follows~~All of the following documentation for the Sub-County:

(A) ~~Submit a copy of the Sub-County's Resolution to participate in a Multi-County ERDS as approved by the Board of Supervisors~~An Application for Sub-County System Certification form # ERDS 0001B (May 2011).

(B) A copy of the Resolution to participate in a Multi-County ERDS as approved by the Sub-County board of supervisors.

(~~B~~C) ~~Submit p~~Proof of fingerprint submission for individuals designated as having a role that requires fingerprinting and a copy of the list of all users with ~~secure and/or authorized access~~Secure Access.

(~~C~~D) ~~Submit a~~A signed and dated Statement of Understanding form # ERDS 0011 (May 2011) declaring under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

Note: Authority cited: Sections 27393, 27393(b)(6), 27394(a), and 27395(b), Government Code. Reference: Sections 27392(a), 27392(b), 27393(b)(2), 27393(b)(6), 27393(b)(10), 27394(a), and 27395(b), Government Code.

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

(a) In order to add or delete individuals from the list of all individuals designated as having Secure Access and/or authorized access to operate the ERDS specified in section 999.165, subdivision (i)(2), the~~The~~ County Recorder shall submit to the ERDS Program a ~~completed~~ Change of ERDS Role form # ERDS 0008 (May 2011) ~~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~~.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27391, 27392, 27393(b)(9), 27394, and 27395(b), Government Code.

§ 999.178. Withdrawal ~~of~~from Certification or from Multi-County ERDS.

(a) ~~A County Recorder choosing to withdraw~~In order to withdraw from ERDS Certification a County Recorder shall submit to the ERDS Program all of the following:

(1) An Application for Withdrawal form # ERDS 0010 (May 2011) ~~with a~~that includes the date for ~~cease~~ceasing ERDS ~~of~~ operation~~/service~~, signed and dated ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(2) ~~Listing~~A listing of all individuals designated as having ~~secure access and/or authorized access~~Secure Access.

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

(4) The withdrawal request shall render the System Certificate of Operation for that County Recorder~~certificate~~ invalid. The withdrawing County Recorder shall cease all ERDS operations as of the cease of operation date ~~noted on the withdrawal application~~listed on the Application for Withdrawal form # ERDS 0010 (May 2011).

(b) ~~In the case of county(ies) withdrawing~~In order to withdraw from a Multi-County ERDS, ~~the Sub-County(ies)~~a Sub-County shall submit ~~the~~an Application for Withdrawal form # ERDS 0010 (May 2011) that includes the date for ceasing ERDS operation, signed and dated with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct to the Lead County. The Lead County shall submit the Sub-County Application for Withdrawal form # ERDS 0010 (May 2011) ~~for submission~~ to the ERDS Program.

(c) ~~If, at a later date, the County Recorder wishes to participate in an ERDS, all initial steps for System Certification shall be required.~~In order to renew ERDS Program certificate at a later date, a County Recorder that withdraws from certification or a Sub-County that withdraws from a Multi-County ERDS must complete all requirements for initial certification pursuant to section 999.166.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), and 27397.5(d)(2), Government Code.

§ 999.190. Computer Security Auditor Application Procedure.

(a) ~~All individuals shall~~An individual must be approved by the ERDS Program prior to ~~entering into contracts~~contracting with a County Recorder~~s to provide auditing services of an ERDS~~ to serve as a Computer Security Auditor.

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

(~~c~~b) An individual applying for approval as a Computer Security Auditor shall ~~comply with~~submit to the ERDS Program all of the following:

(1) ~~Submit a~~An Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013), which shall be dated and signed ~~declaring~~with a declaration under penalty of perjury ~~that~~under the laws of the State of California that all ~~the foregoing~~information contained therein, and all information submitted with the application, is true, correct, and complete~~, and~~; an acknowledgment that ~~a~~ providing any false or dishonest ~~answer to any question~~information in connection with the application may be grounds for denial or subsequent termination or suspension of approval~~. In addition, the individual shall attest to the fact~~; and an attestation that ~~he or she~~the applicant is not an Authorized Submitter, Agent of an Authorized Submitter, or Certified Vendor of ERDS Software as defined in ~~these regulations~~this chapter. The applicant must also indicate on the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) one or more of the following geographical locations he or she is seeking approval for as a Computer Security Auditor:

(A) ~~Check the geographical locations on the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) that they are interested in auditing. The locations are:~~

~~(1)~~ Northern California, which consists of the counties of~~:~~ 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, and Yuba.

(~~2~~B) Central California, which consists of the counties of~~:~~ 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, and Tuolumne.

(~~3~~C) Southern California, which consists of the counties of~~:~~ Imperial, Los Angeles, Orange, Riverside, San Bernardino, Santa Barbara, San Diego, and Ventura.

~~(4) All.~~

(2) ~~Submit documentation with the Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) as follows~~At least one of the following to demonstrate ~~that the individual~~ has met the significant experience criteria required for approval as a Computer Security Auditor:

(A) A copy of ~~their~~the applicant's Certified Internal Auditor certification in good standing 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 (August 2013), and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts for whom the applicant has worked within the last five (5)-year period ~~that~~who can verify the ~~individual~~applicant has ~~had~~ at least two (2) years of experience in the evaluation and analysis of Internet security design~~,~~ and in conducting security testing procedures, and specific experience performing Internet penetration studies~~, or~~.

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

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

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

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

(3) ~~Submit p~~Proof of fingerprint submission.

Note: Authority Cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27393(b)(3), 27393(b)(9), 27394, 27395(a), and 27395(b), Government Code.

§ 999.195. Renewal of Approval.

(a) The certificate of approval issued by the ERDS ~~Certificate of Approval~~program to a Computer Security Auditor shall be renewed prior to expiration in order to remain valid. The ~~certificate holder~~applicant for renewal shall submit~~an Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) indicating renewal, which shall be dated and signed declaring under penalty of perjury that under the laws of the State of California all the foregoing information, and all information submitted with the application is true, correct, and complete, and that a false or dishonest answer to any question 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.~~ to the ERDS Program all of the following:

(1) An Application for Computer Security Auditor Approval form # ERDS 0002 (August 2013) indicating renewal, which shall be dated and signed with a declaration under penalty of perjury under the laws of the State of California that all information contained therein, and all information submitted with the application, is true, correct, and complete; an acknowledgment that providing any false or dishonest information in connection with the application may be grounds for denial or subsequent termination or suspension of approval; and an attestation that the applicant is not an Authorized Submitter, Agent of an Authorized Submitter, or Certified Vendor of ERDS Software as defined in this chapter.

(2) At least one of the following to demonstrate that the applicant has met the significant experience criteria required for renewal of approval as a Computer Security Auditor:

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

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

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

worked within the last five (5)-year period who can verify the applicant has at least two (2) years of experience in the evaluation and analysis of Internet security design and in conducting security testing procedures, and specific experience performing Internet penetration studies.

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

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

(~~g~~b) If the certificate holder fails to comply with the renewal requirements set forth in this provision, the ~~certification~~certificate of approval issued by the ERDS Program shall expire and will no longer be valid~~by operation of the law~~ at midnight on the expiration date stated on the certificate~~, and, render the certificate invalid and all Computer Security Auditor services shall cease~~. The holder of an expired certificate must cease all Computer Security Auditor services. ~~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 individual with a cover letter outlining the process for initial approval.~~ An application for renewal received after the certificate expiration date will be considered an application for initial approval as a Computer Security Auditor.

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

Note: Authority Cited: Sections 27393 and 27394(b), Government Code. Reference: Sections 27392(a), 27393(b)(2), 27393(c), and 27394(b), Government Code.

§ 999.196. Withdrawal ~~of~~from Approval

(a) ~~A Computer Security Auditor choosing to withdraw their approval status~~In order to withdraw from ERDS Program approval, a Computer Security Auditor shall submit to the ERDS Program an Application for Withdrawal form # ERDS 0010 (~~February 2007~~May 2011) that includes a date for terminating ~~operation/~~service, signed and dated ~~declaring~~with a declaration under penalty of perjury under the laws of the State of California that all information contained therein is true and correct.

(b) Upon receipt of the Application for Withdrawal form # ERDS 0010 (~~February 2007~~May 2011), the ERDS Program shall send the applicant a written acknowledgement of the request for withdrawal and notification that the ~~auditor's~~applicant's information has been removed from the listing of Computer Security Auditors posted on the ERDS ~~web~~Program Internet page.

(c) ~~The withdrawal request shall render the certificate invalid. The withdrawing Computer Security Auditor shall cease all ERDS services as of the cease of operation or service date noted on the withdrawal application.~~ As of the service termination date listed on the Application for Withdrawal form # ERDS 0010 (May 2011), the applicant's certificate of approval from the ERDS program shall be invalid, and the applicant must cease all ERDS services.

(d) ~~If at a later date, a Computer Security Auditor wishes to have his or her approval re-instated, the individual shall complete the application process.~~ In order to renew ERDS Program approval at a later date, a Computer Security Auditor who withdraws from ERDS Program approval must complete all requirements for initial approval pursuant to section 199.190.

Authority cited: Section 27393, Government Code.
Reference: Sections 27393(b)(2), 27393(c), 27394(a), and 27394(b), Government Code.

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

(a) To request a replacement certificate of approval or copies of any documents ~~pertaining to~~submitted with ~~their~~his or her application submission, a Computer Security Auditor may submit a Request for Replacement of Certificate and/or Documents form # ERDS 0006 (~~February 2007~~May 2011), signed and dated ~~declaring~~with a declaration 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: Section 27393, Government Code.

Reference: Sections 27393(b)(2), 27393(c), and 27394(a), Government Code.

§ 999.217. Security Audits.

(a) The ERDS Program ~~has the responsibility~~is responsible for oversight and regulation of an ERDS. This responsibility shall be met ~~by~~through the initial system audit, biennial audit, modified system audit, and modified system incident audit, and local inspection process as set forth in this section and in section 999.219.

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

(c) A 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~~2) ensuring ERDS operating procedures are in place and are being followed~~,~~; and ~~4~~3) that the ERDS ~~have~~has 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 Computer Security Auditor has validated that all the requirements of these regulations have been met, including certification by the County Recorder and the ERDS Program that the method of submission allowed under the system will not permit an Authorized Submitter or its employees 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 Computer Security Auditor's findings, the ERDS Program 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~~initial ~~Systems~~system ~~Audit~~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 Computer Security Auditor. A copy of the successful initial system audit report shall be submitted to the County Recorder of a Single-County ERDS or the Lead County of a Multi-County ERDS, which must then submit it to~~the~~ ERDS Program as an attachment to the Application for System Certification form # ERDS 0001A (May 2011). A successful initial system audit report shall be sufficient to meet the ~~1st~~first year audit requirement and shall include, but is not limited to, all of the following:

(1) ~~Description of Deposit~~A description of deposit ~~Materials~~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~~Confirmation of 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 ~~these regulations~~this chapter.

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

(4) ~~Testing and review shall include~~Confirmation that all of the following were included in the audit:

(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 all 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~~Confirmation that the requirements of ~~these regulations~~this chapter are met.

(e) A ~~Biennial~~biennial ~~Audit~~audit ~~and a local inspection are~~is required ~~in alternating years~~ to meet the ongoing oversight ~~of~~ requirements for 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 Computer Security Auditor. A copy of the successful biennial audit report shall be ~~and~~ submitted to the County Recorder of a Single-County ERDS or the Lead County of a Multi-County ERDS, which shall then submit it to the ERDS Program. ~~A local inspection shall be performed by an ERDS Program representative in the alternating years of all Single-County ERDS and the Lead County of a Multi-County ERDS. Sub-Counties will be initially inspected and will then be subject to random scheduled inspections thereafter which shall be completed by an ERDS Program representative. 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 limited to, all of the following:

(1) ~~Description of Deposit Materials~~A 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~~Confirmation of 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 and that the published updates to the standards and guidelines as described in ~~these regulations~~this chapter 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 ~~these regulations~~this chapter.

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

(4) ~~Testing and review shall include~~Confirmation that all of the following were included in the audit:

(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 all 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 that auditable events are collected for audit and that audit data correlates to actual activities.

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

(K) ~~That~~Confirmation that the requirements of ~~these regulations~~this chapter are met.

(~~f~~g) A ~~Modified~~modified ~~System~~system ~~Audit~~audit is required ~~to obtain approval for making a~~for ERDS Program approval of any 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~~performed by a 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.~~ A copy of the successful modified system audit report shall be submitted to the County Recorder of a Single-County ERDS or the Lead County of a Multi-County ERDS, which shall then submit it to the ERDS Program within~~Within~~ fifteen (15) business days of the provisional implementation of the proposed substantive modification~~, 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 # ERDS 0013 (May 2011). A successful modified system audit may satisfy~~not replace~~ the biennial audit requirement when the modified system audit is conducted as a full biennial audit and not limited to the components proposed to be modified. A successful modified system audit report shall include, but is not limited to, all of the following:

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

(2) Demonstration of the ~~ERDS~~substantive modification in its intended production/operational environment.

(3) ~~The audit shall focus on~~Confirmation that the functions of the substantive modification ~~and show~~comply with 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 ~~these regulations~~this chapter.

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

(4) ~~Testing and review shall include~~Confirmation that all of the following were included in the audit:

(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 all 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 that auditable events are collected for audit and that audit data correlates to actual activities.

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

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

(~~g~~h) A ~~Modified System Incident Audit~~modified system incident audit is required to meet the audit requirement resulting from an incident, as defined and described in chapter, that compromises the ~~safety or~~ security of an ERDS~~. Incidents are detailed within these regulations~~. 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~~performed by a Computer Security Auditor ~~and submitted to the County Recorder~~. ~~The County Recorder shall submit a~~A copy of the successful modified system incident audit report shall be submitted to the County Recorder of a Single-County ERDS or the Lead County of a Multi-County ERDS, which shall then submit it to the ERDS Program. A successful modified system incident audit may not replace the biennial audit requirement. A successful modified system incident audit report shall include, but is not limited to, all of the following:

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

(2) Confirmation that the correction to~~The audit shall focus on~~ the cause of the incident of fraud~~, and show~~ complies with 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 and that the published updates to the standards and guidelines as described in ~~these regulations~~this chapter 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 ~~these regulations~~this chapter.

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

(3) ~~Testing and review shall include~~Confirmation that all of the following were included in the audit:

(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 all 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 that auditable events are collected for audit and that audit data correlates to actual activities.

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

(K) That the requirements of ~~these regulations~~this chapter 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 Computer Security Auditor, County Recorder, Board of Supervisors, and District Attorney.~~

~~(C) Maintain reports for statistical purposes.~~

(i) Upon receipt of the modified system incident audit report, the ERDS Program shall: send a written notification within ten (10) business days to the County Recorder acknowledging receipt of the audit report; send a notification of the investigative results and the appropriate action to be taken, if any, to the Computer Security Auditor, County Recorder, Board of Supervisors, and District Attorney; maintain a copy of the report for statistical purposes.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27390(b)(2), 27392(a), 27393(b)(2), 27393(b)(3), 27393(b)(6), and 27394(c)-(f), Government Code.

§ 999.218. Audit Report Format.

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

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

(2) A description of the Computer Security Auditor's methodology.

(3) A section for detailed technical observations and recommendations.

(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.

(7) A copy of the list of all users ~~for secure and/or authorized access~~who have been approved for Secure Access to the ERDS.

Note: Authority cited: Sections 27393 and 27394(c)-(f), Government Code. Reference: Sections 27393(b)(2), 27393(b)(3), 27393(b)(6), 27393(c), and 27394(c)-(f), Government Code.

§ 999.219. 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. All Single-County ERDS and the Lead County of a Multi-County ERDS shall be inspected on an biennial basis. Sub-Counties will be initially inspected and will then be subject to random scheduled inspections thereafter by an ERDS Program representative. 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.~~Local inspections by a representative of the ERDS Program are required to meet the ongoing oversight requirements for an existing certified Single-County ERDS or Multi-County ERDS. A local inspection shall be performed of all Single-County ERDS and the Lead County of a Multi-County ERDS upon initial certification and thereafter biennially. A local inspection shall be performed of a Sub-County of a Multi-County ERDS upon initial certification and thereafter on a randomly scheduled basis.

(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 hardware, software, workstations, and network devices comprising the ERDS, including those located at the offices of Authorized Submitters and/or their Agents, on a mutually agreed upon date.

(c) The ERDS Program representative shall verify all of the following during the local inspection:

(1) An auditable log is being maintained for two (2) years or a computer security audit has taken place within the last 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~~ Computer Security Auditor reports that reference all of the following are being maintained for a period of two (2) years ~~and the following are referenced~~: a list of all ~~secure access~~Secure Access ~~and authorized access~~ users; confirmation that 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 ~~these regulations~~this chapter; ~~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~~transmission of reports and responses 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 to establish the ERDS; any applicable county policies and procedures; ~~the County's Policy and Procedures;~~ a signed Statement of Understanding form # ERDS 0011 (May 2011); a list of all ~~secure access~~Secure Access ~~and authorized access~~ users; a signed Acknowledgement of Responsibilities Form # ERDS 0012 (May 2011); a completed Change of ERDS Role form # ERDS 0008 (May 2011) for individuals that have changed an ERDS role~~(s)~~; the Computer Security Auditor ERDS certificate of approval and contract; the letter of deposit to an approved escrow facility; and the Certified Vendor of ERDS Software certificate of approval and the~~ir~~ contract, if any~~. If internal county resources and/or another public entity are being used to develop an ERDS in lieu of a vendor, it shall be stated in the county resolution granting establishment of an ERDS.~~; and a copy of any certificate of insurance required pursuant to section 999.165, subdivision (e).

(6) For a Multi-County ERDS, that a copy of the following is on file: the contract or agreement with the other county(ies); a list of all ~~secure a~~Secure Access ~~and authorized access~~ users; a signed Acknowledgement of Responsibilities form # ERDS 0012 (May 2011); a completed Change of ERDS Role form # ERDS 0008 (May 2011) for individuals that have changed an ERDS role~~(s)~~; ~~the~~all Sub-County~~(ies)~~ resolutions to participate in the ERDS; the Application for Sub-County System Certification form # ERDS 0001B (May 2011); ~~and~~all ~~the~~ Sub-County~~(ies)~~ Recorder~~'s~~ signed Statement of Understanding forms # ERDS 0011 (May 2011)~~.~~; and any certificate of insurance required pursuant to section 999.165, subdivision (e).

(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~~policy and ~~Security~~security Review review report 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~~program ~~Policy~~policy and ~~Security~~security ~~Review~~review report 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~~ The ERDS Program shall forward a copy of a Sub-County report ~~shall be forwarded~~ to the Lead County.

(g) The ERDS Program representative shall provide an inspection result letter within thirty (30) business days of the inspection date 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~~When an inspection results in a finding that the County Recorder has complied with the requirements of this chapter, the ERDS Program representative shall submit a letter to the County Recorder confirming its compliance ~~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~~. The ERDS Program shall forward a copy of a compliance letter for a Sub-County to the Lead County.

(i) When an inspection results in a finding that the County Recorder has not complied with the requirements of this chapter~~In the case of an inspection resulting in an agency deemed non-compliant with a requirement(s)~~, the ERDS Program representative shall~~:~~ submit a letter to the County Recorder containing notification of the non-compliance. The letter shall list non-compliance issues requiring corrective action and a due date allowing thirty (30) days for correction and response by the County Recorder. The ERDS Program shall forward a copy of a non-compliance letter for a Sub-County to the Lead County.

~~(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 Recorder.~~

(~~2~~1) Upon receipt of the County Recorder's response to the request for corrective action, the ERDS Program representative shall ~~review and~~ determine ~~that~~whether all~~the~~ non-compliance issue~~(s)~~ ~~has~~have been addressed, and shall forward a compliance letter to the County Recorder and/or Sub-County Recorder.

(2) If the ERDS Program representative determines that all non-compliance issues have been addressed, the ERDS Program shall submit a letter to the County Recorder confirming its compliance.

(3) If the ERDS Program representative determines that all non-compliance issues have not been addressed~~In the case of a response not satisfactorily addressing the non-compliance issue(s)~~, 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 specified in the non-compliance letter, 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.~~shall contact the County Recorder, or his or her representative, to inquire about the status. The ERDS Program may grant a two (2)-week extension on the due date for response at its discretion.

(5) If no response is received by the due date specified in the non-compliance letter, or under a two (2)-week extension granted by the ERDS Program, the ERDS Program representative shall issue a letter of ERDS suspension to the County Recorder.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27391, 27393~~(b)(2), 27393(c)~~, 27396(a), and 27396(b)(1), Government Code.

§ 999.220. Incident Reporting.

(a) A reportable incident that compromises the ~~safety or~~ security of an ERDS shall be reported to the ERDS Program by either U.S. Mail or electronic mail.

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

(c) In the case of a Multi-County ERDS, ~~the~~any Sub-County~~(ies)~~ shall report incidents to the Lead County Recorder within two (2) business days.

~~(d) A Fax Transmission Cover Sheet form # ERDS 0007 (May 2011) shall be utilized to notify the ERDS Program of the reportable incident(s).~~

(e~~d~~) After ~~the fax notification has been made~~notifying the ERDS Program of a reportable incident, 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 all of the following: 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 incidents.

(~~f~~e) The detailed incident report shall be forwarded to the ERDS Program, the Computer Security Auditor, District Attorney of all affected counties~~(s)~~, and the~~ir~~ Board of Supervisors of all affected counties within ten (10) business days of the incident~~(s)~~ date. The County Recorder shall maintain the report for a period of two (2) years, and the report shall be subject to review during audits and local inspections.

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

(1) Send ~~a~~ written notification within two (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, Computer Security Auditor, Board of Supervisors of all affected counties, and District Attorney of all affected counties.

(3) Maintain a copy of the report~~s~~ for statistical purposes.

Note: Authority cited: Sections 27393, 27396(a) and 27396(b), Government Code. Reference: Sections 27393(b)(2), 27393(c), 27394(f), 27396(a), and 27396(b), Government Code.

§ 999.221. Suspension and Termination of Certification

(a) System certification may be suspended or terminated. Grounds for suspension or termination shall include, but are not limited to, all of the following:

(1) Unsatisfactory audit findings by a 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~~system ~~Administration~~administration ~~Fee~~fee.

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

(6) Non-compliance with the Statement of Understanding form # ERDS 0011 (May 2011).

(7) For good cause.

Note: Authority cited: Sections 27393, 27396(a) and 27396(b), Government Code. Reference: Sections 27392(a), 27393(b)(2), 27393(c), 27394(c)-(f), 27396(a), and 27396(b), Government Code.

§ 999.223. 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 thirty (30) days of the notification stating justification for the reconsideration. ~~During this time,~~ ~~t~~The County Recorder may not operate the ERDS until the ERDS Program has made a determination on the request for reconsideration.

(b) The ERDS Program shall submit a written determination on the request for reconsideration to the County Recorder within thirty (30) days of receiving the request~~review the request for reconsideration and a determination shall be made in writing to the County Recorder within 30 days~~. A copy of the ~~letter~~determination shall be provided to the Board of Supervisors, the Attorney General, and the District Attorney.

(c) ~~Reinstatement of an ERDS certification that~~If an ERDS system certification has been suspended or terminated because of vulnerabilities, the County Recorder shall provide a ~~Modified System Incident Audit~~modified system incident audit report to the ERDS Program before ~~reinstatement of the~~it may resume ERDS operation. Vulnerabilities include unsatisfactory audit findings by a Computer Security Auditor and/or reported incidents that have been determined to compromise the ~~safety or~~ security of an ERDS.

(d) Reinstatement of an ERDS system certification that has been suspended or terminated because of non-compliance ~~to~~with administrative requirements shall be ~~dependant~~dependent, at the discretion of the ERDS Program, upon ~~responding to and rectifying~~the County Recorder's response and correction action to the reason(s) for suspension or termination. ~~Administrative~~For purposes of this section, 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~~system ~~Administration~~administration ~~Fee~~fee, non-compliance with the Statement of Understanding form # ERDS 0011 (May 2011), and/or good cause.

Note: Authority cited: Sections 27393, 27396(a), and 27396(b)(1), Government Code. Reference: Sections 27392(a), 27393(b)(2), 27393(c), and 27396, Government Code.