State of California
Office of Administrative Law

In re:
Department of Justice

Regulatory Action:

Title 11, California Code of Regulations

Adopt sections:
Amend sections: 999.121, 999.129, 999.133, 999.137, 999.141, 999.143, 999.144, 999.145, 999.146, 999.165, 999.166, 999.168, 999.171, 999.172, 999.173, 999.174, 999.176, 999.178, 999.179, 999.190, 999.191, 999.192, 999.193, 999.195, 999.203, 999.204, 999.206, 999.207, 999.209, 999.210, 999.211, 999.217, 999.219, 999.220, 999.221, 999.223
Repeal sections:

NOTICE OF APPROVAL OF REGULATORY ACTION

Government Code Section 11349.3

OAL File No. 2014-0630-07 SR

This rulemaking action amends regulations in Title 11 of the California Code of Regulations regarding the technology, the security of the technology, and the expertise and reliability of persons involved with the technology of transmitting documents concerning real property transactions pursuant to the Electronic Recording Delivery Act of 2004. The action updates standards of the National Institutes of Standards and Technology and Federal Information Processing Standards which are incorporated by reference in these regulations. The action updates 13 state forms used in the Electronic Recording Delivery System. The action also makes a number of other related changes.

OAL approves this regulatory action pursuant to section 11349.3 of the Government Code. This regulatory action becomes effective on 10/1/2014.

Date: 8/11/2014

Dale P. Mentink
Senior Attorney

For: DEBRA M. CORNEZ
Director

Original: Kamala Harris
Copy: Melan Noble

RESUBMITTAL

STATE OF CALIFORNIA--OFFICE OF ADMINISTRATIVE LAW

NOTICE PUBLICATION/REGULATIONS SUBMISSION

(See instructions on reverse)

STD. 400 (REV. 01-2013)

For use by Secretary of State only

ENDORSED FILED IN THE OFFICE OF

2014 AUG 11 PM 1:40

Debra Bowen

DEBRA BOWEN SECRETARY OF STATE

OAL FILE NUMBERS	NOTICE FILE NUMBER Z-2013-0118-03	REGULATORY ACTION NUMBER 2014-0630-07SR	EMERGENCY NUMBER

For use by Office of Administrative Law (OAL) only

30 PM 3:55

OFFICE OF ADMINISTRATIVE LAW

NOTICE

REGULATIONS

AGENCY WITH RULEMAKING AUTHORITY Department of Justice	AGENCY FILE NUMBER (if any) DOJ-12-008

A. PUBLICATION OF NOTICE (Complete for publication in Notice Register)

1. SUBJECT OF NOTICE	TITLE(S)	FIRST SECTION AFFECTED	2. REQUESTED PUBLICATION DATE
3. NOTICE TYPE □ Notice re Proposed Regulatory Action □ Other	4. AGENCY CONTACT PERSON	TELEPHONE NUMBER	FAX NUMBER (Optional)
OAL USE ONLY	ACTION ON PROPOSED NOTICE □ Approved as Submitted □ Approved as Modified □ Disapproved/ Withdrawn	NOTICE REGISTER NUMBER 2013, 52	PUBLICATION DATE 2/1/2013

B. SUBMISSION OF REGULATIONS (Complete when submitting regulations)

1a. SUBJECT OF REGULATION(S) Electronic Recording Delivery System	1b. ALL PREVIOUS RELATED OAL REGULATORY ACTION NUMBER(S) 2014-0131-02SR

2. SPECIFY CALIFORNIA CODE OF REGULATIONS TITLE(S) AND SECTION(S) (Including title 26, if toxics related)

SECTION(S) AFFECTED (List all section number(s) individually. Attach additional sheet if needed.)	ADOPT
	AMEND See Attached
TITLE(S) 11	REPEAL

3. TYPE OF FILING

□ Regular Rulemaking (Gov. Code §11346)

☒ Resubmittal of disapproved or withdrawn nonemergency filing (Gov. Code §§11349.3, 11349.4)

□ Emergency (Gov. Code, §11346.1(b))

□ Certificate of Compliance: The agency officer named below certifies that this agency complied with the provisions of Gov. Code §§11346.2-11347.3 either before the emergency regulation was adopted or within the time period required by statute.

□ Resubmittal of disapproved or withdrawn emergency filing (Gov. Code, §11346.1)

□ Emergency Readopt (Gov. Code, §11346.1(h))

□ File & Print

□ Other (Specify) ________

□ Changes Without Regulatory Effect (Cal. Code Regs., title 1, §100)

□ Print Only

4. ALL BEGINNING AND ENDING DATES OF AVAILABILITY OF MODIFIED REGULATIONS AND/OR MATERIAL ADDED TO THE RULEMAKING FILE (Cal. Code Regs. title 1, §44 and Gov. Code §11347.1)
August 1, 2013 through August 15, 2013, January 9, 2014 through January 24, 2014, and April 25, 2014 through May 10, 2014

5. EFFECTIVE DATE OF CHANGES (Gov. Code, §§ 11343.4, 11346.1(d); Cal. Code Regs., title 1, §100)

☒ Effective January 1, April 1, July 1, or October 1 (Gov. Code §11343.4(a)) □ Effective on filing with Secretary of State □ §100 Changes Without Regulatory Effect □ Effective other (Specify)

6. CHECK IF THESE REGULATIONS REQUIRE NOTICE TO, OR REVIEW, CONSULTATION, APPROVAL OR CONCURRENCE BY, ANOTHER AGENCY OR ENTITY

☒ Department of Finance (Form STD. 399) (SAM §6660) □ Fair Political Practices Commission □ State Fire Marshal

□ Other (Specify) ________

7. CONTACT PERSON Melan Noble	TELEPHONE NUMBER (916) 322-0908	FAX NUMBER (Optional) (916) 324-5033	E-MAIL ADDRESS (Optional) Melan.Noble@doj.ca.gov

8. **I certify that the attached copy of the regulation(s) is a true and correct copy of the regulation(s) identified on this form, that the information specified on this form is true and correct, and that I am the head of the agency taking this action, or a designee of the head of the agency, and am authorized to make this certification.**

SIGNATURE OF AGENCY HEAD OR DESIGNEE

DATE
6.17.14

TYPED NAME AND TITLE OF SIGNATORY
Nathan R. Barankin, Chief Deputy Attorney General

For use by Office of Administrative Law (OAL) only

ENDORSED APPROVED

AUG 11 2014

Office of Administrative Law

ATTACHMENT TO
STD. 400

REVISED: TITLE 11, DIVISION 1, CHAPTER 18,

ARTICLE 4, SECTIONS: 999.121

ARTICLE 5, SECTIONS: 999.129, 999.133, 999.137, 999.141, 999.143, 999.144, 999.145 and 999.146

ARTICLE 6, SECTIONS: 999.165, 999.166, 999.168, 999.171, 999.172, 999.173, 999.174, 999.176, 999.178, and 999.179

ARTICLE 7, SECTIONS: 999.190, 999.191, 999.192, 999.193, and 999.195

ARTICLE 8, SECTIONS: 999.203, 999.204, 999.206, 999.207, 999.209, 999.210, and 999.211

ARTICLE 9, SECTIONS: 999.217, 999.219, 999.220, 999.221 and 999.223

Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 4. Fingerprinting and Criminal Record Checks

§ 999.121. Fingerprinting and Criminal Record Checks.

…

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

(f) If the ERDS Program is notified of a subsequent arrest and/or disposition, the individual, his or her known employer, the Computer Security Auditor, and the County Recorder shall be notified within 10 business days of the individual's ineligibility for access to an ERDS, if applicable~~,~~.

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

(1) When an individual who was previously approved for an ERDS role that requires fingerprinting, changes roles and/or agencies, changes employment, or is designated additional secure access roles within the same agency; or if an employee or agent of an Authorized Submitter submits to one county and now submits to multiple counties re-fingerprinting is not required. However, for such an individual, proof of fingerprinting shall be provided to the ERDS Program by submission of a Change of ERDS Role form #ERDS 0008 ~~(February 2007),~~(May 2011) consistent with procedures outlined within these regulations.

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

~~(1) Electronic fingerprint submissions. A notarized applicant copy of the Request for Live Scan Services form # BCII 8016ERDS (February 2007) shall be provided as proof of fingerprint submission. If a notarized copy cannot be provided, the individual shall be fingerprinted.~~

~~(2) Manual fingerprint submissions. If an individual initially used the manual method of fingerprinting, the individual shall be fingerprinted.~~

Note: Authority Cited: Sections 27393, 27395(a), 27395(b), 27395(c), 27395(d) and 27395(e), Government Code. Reference: Sections 27393(b), 27393(b)(9) and 27395, Government Code; and Sections 1203.4, 11105 and 11105.2, Penal Code.

…

Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 5. Baseline Requirements and Technology Standards

Note: The preexisting text is set forth below in normal type. The amendments are shown in underline to indicate additions and ~~strikeout~~ to indicate deletions. The symbol "…" means that intervening text not being amended is not shown.

§ 999.129. Standards and Guidelines.

Standards and guidelines contained in these regulations are based on National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) publications including: NIST Special Publication 800-88, Guidelines for Media Sanitization (publication date, September 2006); FIPS 180-~~2~~ 4 Secure Hash Standard (publication date, ~~August 2002 with change notice dated February 2004~~March 2012); FIPS 140-2, Security Requirements for Cryptographic Modules (publication date, May 2001 with a change notice dated, December 2002); FIPS 197, Advanced Encryption Standard (publication date, November 2001); FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC) (publication date, ~~March 2002~~July 2008); NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, ~~April 2006 Version 1.0.2~~August 2013); NIST Special Publication 800-70 Revision 2, ~~Security Configuration Checklists Program for IT Products~~National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date, ~~May 2005~~February 2011);~~.~~ FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013). The ERDS Program shall make available any update, revision or replacement of a reference cited.

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

§ 999.133. Payload Structure, Content and Usage.

…

(e) Multiple digital electronic records or digitized electronic records within the same payload ~~is~~ are allowed; only Secure Access users are authorized to include both Type 1 and Type 2 instruments in the same ERDS payload. ~~however, Type 1 and Type 2 instruments may not be included in the same ERDS payload.~~

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

§ 999.137. Security Requirements for Payload Protection.

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

(1) The ~~RSA~~ Algorithm 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 ~~A~~all ERDS, ~~for~~ 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, ~~T~~the approved hash function ~~approved~~ 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 ~~A~~all ERDS ~~for~~ 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 ~~The~~ 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).

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b) 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 required for Type 1 instruments as follows:

…

(2) For all ERDS certified before January 1, 2015, ~~A~~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, ~~T~~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.

…

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

§ 999.143. ERDS Server Security Requirements.

(a) ERDS that employ 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:

…

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

(A) 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, for all ERDS certified before January 1, 2015, NIST Special Publication 800-70 Revision 2, Security Configuration Checklists Program for IT Products-Guidelines for Checklist Users and Developers (publication date, February 2011). 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, NIST Special Publication 800-70 Revision 2, Security Configuration Checklists Program for IT Products-Guidelines for Checklist Users and Developers (publication date, February 2011).

…

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) 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:

…

(3) For all ERDS certified before January 1, 2015,~~T~~the standard for establishing secure connection is the ~~TLS protocol as~~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 ~~authenticity~~authentication of encrypted ERDS payloads. ~~Each~~ 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).

…

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

§ 999.145. Physical Security.

…

(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:

…

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

…

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.

…

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

…

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

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

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

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

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

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

(11~~3~~) Authentication failures.

(12~~4~~) ERDS accounts locked out and/or disabled due to failed consecutive login attempts. This is an incident and shall be reported if intrusion is suspected.

(13~~5~~) Auditable events overwrite other logged events. This is an incident and shall be reported if intrusion is suspected.

(14~~6~~) Auditable events cannot be logged. This is an incident.

(15~~7~~) Logs consume 95% or more of the storage space allocated for logging. This is an incident.

(16~~8~~) Logs cannot be safely stored. This is an incident.

(17~~9~~) For Type 1 only, ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not. This is an incident only if not authorized and shall be reported if fraud is suspected.

(~~20~~18) For Type 1 only, hardware or software configuration changes. This is an incident only if not authorized and shall be reported.

(~~21~~19) Unique name of the ERDS payload. This is an incident only if out of sequence.

(~~22~~20) Dates and times the ERDS payload was submitted, retrieved or, when applicable, returned. This is an incident only if the dates and times are not current.

(~~23~~21) Identity of the individual, who submitted, retrieved or, when applicable, returned the ERDS payload. This is an incident only if not authorized.

(~~24~~22) Name of the organization that the individual represented while submitting, retrieving or, when applicable, returning the ERDS payload**.** This is an incident only if not authorized.

(~~25~~23) For Type 1 only, a transmission failure.

(~~26~~24) For Type 1 only, a storage failure.

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

(~~28~~26) A hash failure. This is an incident and shall be reported if fraud is suspected.

(~~29~~27) A validity check failure. This is an incident and shall be reported if fraud is suspected.

(~~30~~28) Type 1 or Type 2 instrument submitted unencrypted. This is an incident and shall be reported.

(~~31~~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.

(~~32~~30) Type 1 instrument submitted via an Authorized Access ERDS. This is an incident and shall be reported if fraud is suspected.

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

(~~34~~31) Unauthorized components that draw data or images from sources external to the digital electronic record or digitized electronic record. This is an incident and shall be reported if intrusion is suspected.

(~~35~~32) Unauthorized transactions submitted via ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2. This is an incident and shall be reported if fraud is suspected.

(~~36~~33) For Type 1 only, server failures, including, but not limited to, hardware, software, and network component failures, that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(~~37~~34) Events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected.

(~~38~~35)For Type 1 only, unauthorized changes to the ERDS operational configuration. This is an incident and shall be reported if fraud or intrusion is suspected.

(~~39~~36) For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(~~40~~37) For Type 1 only, events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected.

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

(~~42~~38) Inability to obtain and employ up-to-date anti-malware software.

(~~43~~39) Inability to obtain and employ cryptography, including hashing, encryption and decryption. This is an incident and shall be reported.

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

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

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

(40~~7~~) Inability to obtain and employ the most up-to-date patches and hot-fixes.

(41~~8~~) Unauthorized access or changes to storage media, and improper sanitization of storage media. This is an incident and shall be reported if compromise is suspected.

(42~~9~~) Any other event that compromises the safety or security of an ERDS. This is an incident and shall be reported.

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

Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 7. Computer Security Auditor

§ 999.190. Computer Security Auditor Application Procedure.

…

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

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

(1) Submit an Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013), 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.

(A) Check the geographical locations on the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) that they are interested in auditing. The locations are:

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

…

(2) Submit documentation with the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) as follows to demonstrate that the individual has met the significant experience criteria required for approval as a Computer Security Auditor:

(A) A copy of their Certified Internal Auditor certification from the Institute of Internal Auditors for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(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

(B) A copy of their Certified Information Systems Auditor certification from the Information Systems Audit and Control Association for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(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

(C) A copy of their Certified Fraud Examiner certification from the Association of Certified Fraud Examiners for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 Computer Security Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, or

(D) A copy of their Certified Information Systems Security Professional certification from the International Information Systems Security Certification Consortium for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 Computer Security Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, or

(E) A copy of their Global Information Assurance Certification from the SysAdmin, Audit, Networks Security Institute for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 Computer Security Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies.

(3) Submit 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.

§ 999.191. Approval of Application.

…

(2) An ERDS Certificate of Approval which authorizes the individual to contract with a County Recorder to perform the duties of a Computer Security Auditor. The certificate shall remain in effect for three years unless terminated based on a subsequent arrest and/or disposition.

…

Authority cites: Section 27393 Government Code.
Reference: Sections 27392(a) and 27394, Government Code.

...

§ 999.192. Incomplete Application.

…

(b) The applicant shall have 90 days to respond, after which the application shall be considered denied. The denial may not prohibit the submission of an Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) at a later date.

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

§ 999.193. Denial of Application.

(a) The Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) may be denied for good cause. Good cause shall be deemed to exist when the applicant does not satisfy the qualifications or system requirements of these regulations, it is necessary to protect the public interest, protect the integrity of records, or to protect homeowners from financial harm.

(b) Denied applications shall be returned to the individual with a written explanation for the denial. The denial may not prohibit the resubmission of an Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) at a later date.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(c), 27394 and 27395(a), Government Code.

§ 999.195. Renewal of Approval.

(a) The ERDS Certificate of Approval shall be renewed prior to expiration in order to remain valid. The certificate holder shall submit an Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(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.

(b) A copy of their Certified Internal Auditor certification from the Institute of Internal Auditors for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(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

(c) A copy of their Certified Information Systems Auditor certification from the Information Systems Audit and Control Association for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 (May 2011) listing reference contacts within the last 5-year period that can verify the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, or

(d) A copy of their Certified Fraud Examiner certification from the Association of Certified Fraud Examiners for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 (February 2007) Computer Security Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, or

(e) A copy of their Certified Information Systems Security Professional certification from the International Information Systems Security Certification Consortium for which they are in good standing attached to the Application for ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 Computer Security Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies, or

(f) 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 ~~DOJ~~ Computer Security Auditor Approval form # ERDS 0002 ~~(February 2007)~~(August 2013) and a completed ~~Attachment to ERDS 0002 Computer Security~~

~~Auditor Significant Experience~~ Reference(s) for ERDS Computer Security Auditor form # ERDS 0004 ~~(February 2007)~~(May 2011) listing reference contacts within the last 5-year period that can verify ~~that~~ the individual has had at least 2 years of experience in the evaluation and analysis of Internet security design, in conducting security testing procedures, and specific experience performing Internet penetration studies.

...

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

Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 8. Vendor of Electronic Recording Delivery System Software

§ 999.203. Certification Application Procedure.

…

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

(1) Submit an Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011), which shall be dated and signed declaring under penalty of perjury that under the laws of the State of California all the foregoing information, and all information submitted with this application is true, correct, and complete, and that a false or dishonest answer to a question may be grounds for denial or subsequent termination or suspension of certification. In addition, the individual shall attest to the fact that the ERDS software, at the time of development, will meet all of the audit and testing requirements as contained within these regulations, and acknowledges that ERDS Program's issuance of the Vendor of ERDS Software Certificate shall include a "disclaimer" stating that the software is not being approved as to its ability to serve/function in an ERDS operational environment nor that it will meet all County Recorder's requirements, only that the Vendor has stated that it will meet all of the audit and testing requirements as contained within these regulations as of the date of the issued certificate.

(2) Submit documentation with the Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) as follows, to demonstrate that they have met the reference or service agreement required to be certified as a Vendor of ERDS Software:

(A) Provide 3 best references within the last 5 years for software products or development of equivalent technology, complexity and size of an ERDS. At least 1 reference shall be for a project using document-imaging technology. Provide this information on the Attachment to ERDS 0003 Vendor Application Form for Reference(s) form # ERDS 0009 ~~(February 2007)~~(May 2011), or

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), 27393(b)(7), 27393(c) and 27397(b), Government Code.

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

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

(1) An ERDS Acknowledgment of Responsibilities form # ERDS 0012 ~~(February 2007)~~(May 2011) shall be signed and kept on file by the County Recorder for all vendor employees and/or vendor contract employees for review during audits and local inspections.

(2) The Vendor of ERDS Software shall notify the County Recorder of any addition or deletion of vendor employees and/or vendor contract employees. The County Recorder shall maintain a list of those individuals and their roles which shall be subject to audit and local inspection. The County Recorder shall submit to the ERDS Program a completed Change of ERDS Role form # ERDS 0008 ~~(February 2007)~~(May 2011) indicating addition or deletion of vendor employees and/or vendor contract employees.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(7), 27393(c) and 27395(b), Government Code.

§ 999.206. Incomplete Application.

(a) An incomplete Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) shall be returned to the applicant with a written explanation for the return and further instructions on resubmission. The application shall be deemed incomplete when:

…

(b) The applicant shall have 90 days to respond, after which the application shall be considered denied. The denial may not prohibit the submission of an Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) at a later date.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(7), 27393(c), 27395(b) and 27397(b), Government Code.

§ 999.207. Denial of Application.

(a) The Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) may be denied for good cause. Good cause shall be deemed to exist when the applicant does not satisfy the qualification or system requirements of these regulations, it is necessary to protect the public interest, protect the integrity of records, or to protect homeowners from financial harm.

(b) Denied applications shall be returned to the individual with a written explanation for the denial. The denial may not prohibit the submission of an Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) at a later date.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(7), 27393(c) and 27395(b), Government Code.

§ 999.209. Renewal of Certification.

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

(1) An Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) indicating renewal.

…

(3) Submit documentation with the Application for Vendor of ERDS Software Certification form # ERDS 0003 ~~(February 2007)~~(May 2011) as follows, to demonstrate that they have met the reference or service agreement required to be certified as a Vendor of ERDS Software:

(A) Provide 3 best references within the last 5 years for software products or development of equivalent technology, complexity and size of an ERDS. At least 1 reference shall be for a project using document-imaging technology. Provide this information on the Attachment to ERDS 0003 Vendor Application Form for Reference(s) form # ERDS 0009 ~~(February 2007)~~(May 2011), or

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(7) and 27393(c), Government Code.

§ 999.210. Withdrawal of Certification.

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

(1) An Application for Withdrawal form # ERDS 0010 ~~(February 2007)~~(May 2011) with a date for cease of operation/service signed and dated declaring under penalty of perjury under the laws of the State of California that all information is true and correct. Submit to the ERDS Program.

(2) A list of all vendor employees and/or vendor contract employees designated as having a role that requires fingerprinting shall be submitted to the County Recorder and a copy attached to the Application for Withdrawal form # ERDS 0010 ~~(February 2007)~~(May 2011).

…

(b) Upon receipt of the Application for Withdrawal form # ERDS 0010 ~~(February 2007)~~(May 2011), the ERDS Program shall send a written acknowledgement of the request for withdrawal.

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), 27393(b)(7) and 27393(c), Government Code.

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

(a) To request a replacement certificate or copies of a document pertaining to their application submission, a Vendor of ERDS Software may submit a Request for Replacement of Certificate and/or Documents form # ERDS 0006 ~~(February 2007)~~(May 2011), signed and dated declaring under penalty of perjury under the laws of the State of California that the requested certificate and/or documents pertains to his or her application submission.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), 27393(b)(7) and 27393(c), Government Code.

Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 9. Audits and Oversight

§ 999.217. Security Audits.

…

(d) The ERDS Initial System Audit is a full system audit and is required to obtain initial system certification. "Initial" is defined as the "first time" application for a certification of an ERDS for either a Single-County or a Multi-County ERDS. This audit shall be performed prior to activating an ERDS for production and operation and shall be completed by a Computer Security Auditor. A copy of the successful initial system audit report shall be submitted to the ERDS Program as an attachment to the Application for System Certification form # ERDS 0001A ~~(February 2007)~~(May 2011). A successful initial system audit shall be sufficient to meet the 1st year audit requirement and shall include, but is not limited to, all of the following:

…

(e) A Biennial Audit and a local inspection are required in alternating years to meet the ongoing oversight of an existing certified Single-County ERDS or a Multi-County ERDS. The biennial audit is a full system audit and shall be performed in the production and operational environment and shall be completed by a Computer Security Auditor and submitted to the County Recorder. 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 ~~and~~which shall be completed by an ERDS Program ~~staff~~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:

…

(f) A Modified System Audit is required to obtain approval for making a substantive modification to an existing certified Single-County ERDS or a Multi-County ERDS. A modified system audit shall pertain to only the components that are proposed to be modified and/or changed in the production environment and shall be performed prior to activating the modification and/or change in the ERDS operational environment. This modified system audit shall be completed by a Computer Security Auditor and submitted to the County Recorder. Upon receipt of the successful modified system audit by the County Recorder, the County Recorder may place the proposed substantive modification in the production environment on a provisional basis. Within 15 business days of the provisional implementation, a copy of the successful modified system audit report shall be submitted to the ERDS Program as an attachment to an Application for a Request for Approval of Substantive Modification(s) form # ERDS 0013 ~~(February 2007)~~(May 2011). A successful modified system audit may not replace the biennial audit requirement. A modified system audit report shall include, but is not limited to, all of the following:

…

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.

§ 999.219. 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.

(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, ~~processes~~ on a mutually agreed upon date.

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

…

(5) For a Single-County ERDS, that a copy of the following is on file: the County's System Certificate of Operation; the County's Resolution; the County's Policy and Procedures; a signed Statement of Understanding form # ERDS 0011 ~~(February 2007)~~(May 2011); a list of all secure access and authorized access users; a signed Acknowledgement of Responsibilities Form # ERDS 0012 ~~(February 2007)~~(May 2011); a completed Change of ERDS Role form # ERDS 0008 ~~(February 2007)~~(May 2011) for individuals that have changed an ERDS role(s); the Computer Security Auditor ERDS certificate and contract; the letter of deposit to an approved escrow facility; and the Vendor of ERDS Software certificate and their contract, if any. If internal 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.

(6) For a Multi-County ERDS, that a copy of the following is on file: the contract or agreement with other county(ies); a list of all secure access and authorized access users; a signed Acknowledgement of Responsibilities form # ERDS 0012 ~~(February 2007)~~(May 2011); a completed Change of ERDS Role form # ERDS 0008 ~~(February 2007)~~(May 2011) for individuals that have changed an ERDS role(s); the Sub-County(ies) resolution; the Application for Sub-County System Certification form # ERDS 0001B ~~(February~~

~~2007)~~(May 2011); and the Sub-County(ies) Recorder's signed Statement of Understanding form # ERDS 0011 ~~(February 2007)~~(May 2011).

…

(g) The ERDS Program representative shall provide an inspection result letter within ~~10~~30 business days of the inspection date to the County Recorder or his or her representative.

…

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

§ 999.220. Incident Reporting.

…

(d) A Fax Transmission Cover Sheet form # ERDS 0007 ~~(February 2007)~~(May 2011) shall be utilized to notify the ERDS Program of the reportable incident(s).

…

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:

…

(6) Non-compliance with the Statement of Understanding form # ERDS 0011 ~~(February 2007)~~(May 2011).

…

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.

…

(d) Reinstatement of an ERDS certification that has been suspended or terminated because of non-compliance to administrative requirements shall be dependent upon responding to and rectifying the reason for suspension or termination. Administrative requirements include failure to respond to a notice of corrective action for a non-compliance issue(s) as a result of local inspection, failure to comply with the audit and local inspection schedule, non-payment of a County's proportionate cost of the System Administration Fee, non-compliance with the Statement of Understanding form # ERDS 0011 ~~(February 2007)~~(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.