

**State of California
Office of Administrative Law**

In re:

Department of Justice

Regulatory Action:

**Title 11, California Code of
Regulations**

**Amend sections: 999.121, 999.129,
999.133, 999.137, 999.139, 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.**

**DECISION OF DISAPPROVAL OF
REGULATORY ACTION**

Government Code Section 11349.3

OAL File No. 2014-0131-02SR

DECISION SUMMARY

On January 31, 2014, the Department of Justice (Department) submitted to the Office of Administrative Law (OAL), this rulemaking action which concerns the technology, the security of the technology, and the reliability and expertise of the individuals involved in electronic transmission of documents necessary for real property ownership change transactions under the Electronic Recording Delivery Act (ERDA) and through the Electronic Recording Delivery System (ERDS). The action updates the editions of certain National Institutes of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) documents which are incorporated by reference in these regulations. The action also updates thirteen forms used by the Department in administration of the ERDS because of the reorganization of the Department and the ERDS program becoming a separate Division within the Department.

OAL disapproved the proposed amended regulations for failure to comply with the clarity standard of the California Administrative Procedure Act (APA) and a number of procedural requirements of the APA. The reasons for the disapproval are summarized below:

A. the proposed regulations fail to comply with the clarity standard of Government Code sections 11349(c) and 11349.1(a)(3) and Title 1 California Code of Regulations (CCR) section 16(a); and

B. the agency failed to comply with various procedural requirements of the APA and its implementing regulations by failing to include:

(1) in the record - a statement regarding the mailing of the notice of the proposed action pursuant to Government Code section 11346.4(a) and Title 1 CCR section 86;

(2) in the record - a Final Statement of Reasons which contained all required alternatives determinations pursuant to Government Code 11346.9(a)(4);

(3) in the record - a statement regarding the mailing recipients, if any, of the Department's August 2013 and January 2014 notices of revisions to the text of the regulations pursuant to Government Code section 11347.3(b)(9) and Title 1 CCR section 44;

(4) with the text of the proposed regulations - copies of all documents, not reasonably available to the public from a commonly known or identified source, which are incorporated by reference by the regulations pursuant Title 1 CCR section 20(d);

(5) text of the proposed regulations which is free of mistakes, track changes, and underlining/strikeout errors.

All issues must be resolved prior to OAL approval of any resubmission of these regulations. Upon resubmission, OAL reserves the right to review these regulations for compliance with all standards of Government Code section 11349.1(a) and all procedural requirements of the APA.

BACKGROUND

The Department conducted this rulemaking action primarily to update and improve the regulations governing the process of electronic transmission of documents related to real property ownership change transactions under the ERDA. The ERDA created a system to electronically deliver, record, and then return instruments affecting real property in California. Under the current regulatory system, two types of documents (Type 1 and Type 2) cannot be submitted or returned within the same ERDS payload. Type 1 documents are those affecting rights, title, or interest in real property. Type 2 documents are instruments of re-conveyance, substitutions of trustees, or assignments of deeds of trust. Although these documents must be recorded together, the current regulations require corresponding documents to be sent separately. In addition to this updating of the regulations, the Department also proposed the updating of the editions

of certain NIST and FIPS documents which contain standards that ERDS participants must comply with and which are incorporated by reference in the proposed regulations. The Department proposed several other amendments to the regulations to strengthen the security of the ERDS and the qualifications of the individuals who operate it and to streamline this system. The Department also updated 13 of its forms to reflect the reorganization of the Department and the creation of a new Division within the Department for the ERDS program.

DISCUSSION

Any regulation amended or adopted by a state agency through its exercise of quasi-legislative power delegated to it by statute to implement, interpret, or make specific the law enforced or administered by it, or to govern its procedure, is subject to the APA unless a statute expressly exempts the regulation from APA review. Government Code sections 11340.5 and 11346. OAL reviews regulatory actions for compliance with the standards for administrative regulations in Government Code section 11349.1. Generally, to satisfy the standards, a regulation must be legally valid, supported by an adequate record, and easy to understand. In its review, OAL may not substitute its judgment for that of the rulemaking agency with regard to the substantive content of the regulation. OAL review is an independent executive branch check on the exercise of rulemaking powers by executive branch agencies and is intended to improve the quality of regulations that implement, interpret, and make specific statutory law, and to ensure that required procedures are followed in order to provide a meaningful opportunity for public comment on regulations before they become effective.

A. Clarity.

In adopting the APA, the Legislature found that the language of many regulations was unclear and confusing to persons who must comply with the regulations. Government Code section 11340(b). Government Code section 11349.1(a)(3) requires that OAL review all regulations for compliance with the clarity standard. Section 11349(c) of the Government Code defines "clarity" to mean "...written or displayed so that the meaning of the regulations will be easily understood by those persons directly affected by them." Moreover, it shall be presumed that a regulation does not comply with the clarity standard if any of the following conditions exist: the regulation can, on its face, be reasonably and logically interpreted to have more than one meaning; the regulation uses terms which do not have meanings generally familiar to those directly affected by the regulation and those terms are not defined in the regulation or the governing statute; the regulation uses language incorrectly; or the regulation does not use citation styles which clearly identify published material cited in the regulation. Title 1 CCR section 16(a). As a result of its review, OAL found that a number of proposed provisions failed to meet the clarity standards of Government Code section 11349(c) and/or section 16(a) of Title 1 of the California Code of Regulations.

(1) Proposed sections 999.139(b), 999.141(a)(2), 999.141(a)(3), 999.143(a)(8), and 999.144(a)(3).

In these proposed subdivisions, the Department requires compliance with a revised FIPS standard but the provisions are not clear as to which FIPS standard must be complied with. If it can be assumed that the standard required is the standard or standards mentioned in these subdivisions, the standards mentioned are NIST standards, not FIPS, with the exception of section 999.144(a)(3) which lists both NIST and FIPS standards. The Department must clarify which standard or standards it is requiring Certified ERDS to comply with in each of these subdivisions.

(2) Proposed sections 999.137(a), 999.137(b), 999.137(c), 999.137(d), 999.139(b), 999.141(a)(2), 999.141(a)(3), 999.143(a)(8), 999.144(a)(3), and 999.144(a)(4).

The proposed subdivisions raise several clarity problems.

First, all proposed subdivisions require compliance with “the revised FIPS [or NIST] standard” but none identifies that standard specifically. The provisions are unclear because a regulated entity must assume that the required revised standard is the FIPS or NIST standard mentioned previously or subsequently in the subdivision. Moreover, regarding proposed section 999.144(a)(3), both NIST and FIPS standards are mentioned previously in the subdivision, but only compliance with a FIPS standard is required. In these subdivisions, the Department must specify which FIPS and/or NIST standard(s) Certified ERDS must comply with.

Second, all proposed subdivisions use the phrase “the revised...standard.” This phrase is unclear in all instances. In, for example, proposed section 999.137(b), if it can be assumed that the required standard is the Secure Hash Algorithm defined in FIPS 180-4, Secure Hash Standard (publication date, March 2012), it is unclear if the phrase “the revised FIPS standard” is a reference to this FIPS standard as it was revised in March of 2012, or to this standard as it may be revised after March of 2012, which would constitute a prospective incorporation by reference and requirement to comply with a yet-to-be-developed revised standard. Each of these ten instances of the use of the phrase “the revised” must be changed to instead specify which standard and which revision of that standard Certified ERDS must comply with.

(3) Proposed sections 999.137(a), 999.137(b), 999.137(c), 999.137(d), 999.139(b), 999.141(a)(2), 999.141(a)(3), 999.143(a)(8), 999.144(a)(3), 999.144(a)(4), and 999.145(b).

In ten proposed subdivisions, the Department has introduced the new term “Certified ERDS” which is not specifically defined. The introduction of this undefined new term makes references to “all ERDS,” in four of these subdivisions and in section 999.145(b), and references to “ERDS,” in the remaining six subdivisions, as well as references to “all ERDS” or “ERDS” elsewhere in Article 5, unclear.

For example, section 999.137(b) provides:

All ERDS for either Type 1 or Type 2 instruments shall use hashing to protect the integrity of ERDS payloads. The hash function approved for ERDS payloads is the Secure Hash Algorithm defined in FIPS 180-4~~2~~, Secure Hash Standard (publication date, March 2012), ~~August 2002 with change notice dated February 2004~~), using a message digest size of at least 224 bits. Certified ERDS shall comply with the revised FIPS standard within 12 months... [presumably a reference to FIPS 180-4 mentioned above]

It is unclear who Certified ERDS is as compared to all ERDS, and whether Certified ERDS is a new subset of all ERDS. It is unclear whether only Certified ERDS must comply with the FIPS standard for hashing and whether non-Certified ERDS (assuming that "all ERDS" includes both Certified and non-Certified ERDS) may use some other standard for hashing and what that standard is. In the alternative, if it can be assumed that all ERDS must comply with FIPS 180-4, it is unclear whether only Certified ERDS are required to comply within 12 months and other ERDS within some other period of time.

Section 999.141(a)(2), for example, provides:

(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:

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

(2) Authentication assurance shall meet Level 3 or higher, as defined by the NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, April 2006 Version 1.0.2 August 2013). Certified ERDS shall comply with the revised FIPS standard within 12 months... [presumably a reference to the NIST standard stated in the first sentence of this paragraph]

(3) The token methods described by the NIST may be used, provided that authentication assurance Level 3 or higher, as defined by the NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, April 2006 Version 1.0.2 August 2013). Certified ERDS shall comply with the revised FIPS standard within 12 months... [presumably a reference to the NIST standard stated in the first sentence of this paragraph]

It is unclear who Certified ERDS is as compared to ERDS, and whether Certified ERDS is a new subset of ERDS. It is unclear whether the references to Certified ERDS in subdivisions (a)(2) and (a)(3) qualify subdivision (a) such that only Certified ERDS must comply with the NIST 800-63-2 standard for authentication security and non-Certified

ERDS need only comply with subdivision (a)(1). In the alternative, if it can be assumed that ERDS must comply with subdivisions (a)(1) through (a)(3), it is unclear whether only Certified ERDS are required to comply with subdivisions (a)(2) and (a)(3) within 12 months and non-Certified ERDS within some other period of time.

The Department must clarify the use of the terms "ERDS," "all ERDS," and "Certified ERDS" in these subdivisions and define these terms or specify any compliance distinctions that exist among them.

(4) Proposed sections 999.137(a), 999.137(b), 999.137(c), 999.137(d), 999.139(b), 999.141(a)(2), 999.141(a)(3), 999.143(a)(8), 999.144(a)(3), and 999.144(a)(4).

These subdivisions all require Certified ERDS to comply with a revised FIPS or NIST standard "within 12 months of the effective date of this amended regulation." It is unclear when this 12-month compliance period would begin to run. All of these regulations will become "amended" regulations if they are amended, but amendment of the regulations will not alter the effective dates of these amended regulations. All of these regulations have an effective date of July 31, 2007. The Department cannot require retroactive compliance within 12 months of July 31, 2007. If the Department intended to require compliance within 12 months of the effective date of *the amendments* to these regulations, amending the regulations accordingly would nevertheless leave the regulations unclear, because, as time goes by and subsequent amendments occur, it would be unclear which amendment made the relevant changes to the text for purposes of selecting an effective date from which to measure 12 months for compliance with those changes. The Department must clarify these subdivisions by specifying a date from which the 12-month compliance period will be measured.

(5) Proposed section 999.143(a)(8).

Proposed section 999.143(a)(8) provides as follows:

(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. Certified ERDS shall comply with the revised FIPS [presumably, the Department intended "NIST" not "FIPS" here] standard within 12 months of the effective date of this amended regulation. Any extensions require written justification for review by the ERDS Program. Such an update is to be considered a substantive modification. The County Recorder shall ensure that all county servers used for ERDS are "hardened" according to one of the following checklists or guidelines:

(A) NIST Special Publication 800-70 Revision 2, Security Configuration Checklist Program for IT Products-Guidelins for Checklist Users and Developers (publication date, February 2011 ~~May 2005~~).

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

Regarding the second sentence of paragraph (8), it is OAL's understanding that Certified ERDS includes County Recorders' Offices. The second sentence of paragraph (8), therefore, requires County Recorders' Offices, as Certified ERDS, to comply with NIST Special Publication 800-70. However, the last sentence of paragraph (8) allows counties to harden county servers according to either: (A) NIST Special Publication 800-70...or (B) Manufacturer's recommended guidelines. The second sentence, therefore, conflicts with the last sentence and creates the potential for two interpretations of the paragraph.

B. Procedural Requirements of the APA.

In the conduct of this rulemaking action, the Department failed to comply with various procedural requirements of the APA as follows:

(1) The Department failed to include in the record of the rulemaking proceeding a statement confirming the mailing of its Notice of Proposed Action to persons and entities specified by Government Code section 11346.4(a)(1)-(4) pursuant to Title 1 CCR section 86.

(2) The Department failed to include in its Final Statement of Reasons two of the required alternatives determinations [(1) more effective, and (2) more cost effective and equally as effective] which are required by Government Code section 11346.9(a)(4).

(3) The mailing statements for the August 1, 2013 and January 9, 2014 availability of modified text fail to include either a statement, pursuant to section 44(c) of Title 1 of the California Code of Regulations, indicating that the Department had no one to whom to mail these notices, or, in the alternative, a statement indicating that the Department mailed these notices to, perhaps, all those persons to whom it mailed its original notice of proposed action as specified by Government Code section 11346.4(a)(1) through (4). The statements are, therefore, ambiguous as to what occurred regarding the mailing of these notices of the availability of revised texts.

(4) The Department failed to include with the text of the proposed regulations for filing with the Secretary of State copies of all FIPS and NIST documents which it is incorporating by reference pursuant to section 20(d) of Title 1 of the California Code of Regulations. Missing from the text are copies of: FIPS 180-4 Secure Hash Standard (publication date, March 2012); NIST Special Publication 800-63-

2, Electronic Authentication Guideline (publication date, August 2013); and FIPS 186-4 Digital Signature Standard (DSS) (publication date, July 2013).

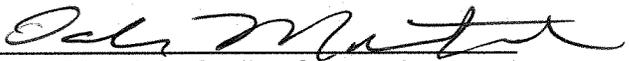
(5) OAL also notes that the text of the proposed regulations contains a number of mistakes, track changes, and underlining and strikeout illustration errors.

All items listed above shall be corrected in any resubmission of this rulemaking action to OAL for review.

CONCLUSION

For the foregoing reasons, OAL disapproved the above-referenced rulemaking action. Pursuant to Government Code section 11349.4(a), the Department may resubmit revised regulations within 120 days of its receipt of this Decision of Disapproval. The Department shall make all substantial regulatory text changes, which are sufficiently related to the original text, available for at least 15 days for public comment pursuant to Government Code section 11346.8.

Dated: March 24, 2014


Dale Mentink, Senior Counsel

For: DEBRA M. CORNEZ
Director

Original: Kamala Harris
Copy: Melan Noble