# INITIAL STATEMENT OF REASONS

**California Code of Regulations**
**Title 11. Law**
**Division 1. Attorney General**
**Chapter 17. ERDS**

## A. Summary of Legislation

The legislation being implemented, AB 578, is set forth and described in the Informative Digest/Policy Statement Overview. (Stats.2004, ch.621, § 2.)

## B. Section-by-Section Analysis

### Article 1. Scope

**§ 100 Purpose.**

This section introduces the legislative history and directives to generate the regulations.

**§ 101 ERDS Documentation.**

This section ensures that an individual's right to privacy is enforced and that confidential information provided on documentation submitted to the ERDS Program is protected from the threat of potential risk in the indiscriminate collection, maintenance, and dissemination of information and the lack of effective laws and legal remedies.

### Article 2. Definitions

**§ 200 Definitions.**

For the purposes of this Chapter, this section provides definitions of commonly used terms and acronyms.

Definitions 1, 3, 5, 8, 21, 27, 32, 46, 50, describe the various parties that shall be involved with the development, establishment, maintenance and oversight of an ERDS. These definitions are necessary to clarify responsibility, authority, and restrictions if any.

Definitions 14, 16, 17, 23, 24, 31, 33, 35, 37, 39, 43, 48 are acronyms that define titles, methods, standards used throughout this chapter. Each acronym spells out the word form and are commonly recognized and understood by law enforcement staff, local government staff, and the information technology industry.

Definition 2 is included to provide reference to the guidelines currently in place for an Approved Escrow Company. As required by the legislation, this Chapter shall establish the requirements for placement of a copy of the operating system source code, compilers, and all related software associated to an ERDS prior to its first use.

Definitions 4, 7, 9, 10, 18, 22, 36, 41, 51 describe different levels of access to an ERDS dependant upon the role an individual has been granted. These provisions are necessary to provide the level of security required for the different types of documents being processed electronically.

Definitions 11 and 13 define the origin of documents that shall be transmitted via an ERDS. The distinction is necessary so that it is understood that there are restrictions and specific guidelines for the submission of electronic documents as outlined in this Chapter.

Definitions 6, 12, 19, 20, 30, 42, 44, 45, 52 are commonly used terms by the information technology industry. It is necessary to identify them within this Chapter as relating to an ERDS because of the possibility of other applications being sent and/or received electronically.

Definitions 25, 26, 29, 38, 40 are common terms that are used in these regulations that relate a specific action, function or description. These definitions are necessary to ensure that the terms are being interpreted by those associated with the operation, maintenance, and oversight in relationship to an ERDS.

Definitions 34 and 47 define changes made to an established ERDS that would or would not impact the daily functionality of a system. It is necessary to identify those modifications so that it is understood when security testing shall be conducted in order to maintain a secure environment for the transmission of electronic records.

Definition 15 employs a term common to the real estate industry. It is necessary for the development of an ERDS to allow for the collection of data as outlined in existing specifications for signatures requiring a notary's seal or stamp.

Definition 28 identifies the acceptable method of electronic submission of fingerprints. As a requirement of this Chapter, individuals with specific roles

associated with an ERDS shall require fingerprint background checks. Penal Code section 11077.1 mandates the Department of Justice only accept electronically transmitted fingerprint images from regulatory entities performing background investigations.

Definition 49 is included as a requirement of the legislation and is commonly understood by County Recorders as a term for data collected and used in the document recording process. A County Recorder shall decide on the content of indexing information and shall ensure that an established ERDS is capable of including the data.

## Article 3. Fees

### § 300 Vendor of ERDS Software Fees.

AB 578 authorizes the Attorney General to charge a fee directly to a vendor seeking approval of software and other services as part of an ERDS. This section establishes and identifies those fees to be charged for an initial certification and a renewal certification.

### § 301 System Administration Fee.

As required by AB 578, a County Recorder choosing to establish an ERDS shall, upon approval by their Board of Supervisors, pay for the direct cost of regulation and oversight. Because participation is voluntary, a method of determining a county's proportionate share of a current years cost has been developed. This section explains the method of calculating a county's proportionate share which has been named the System Administration Fee.

## Article 4. Fingerprinting and Criminal Records Checks

### § 400 Fingerprinting and Criminal Records Checks.

All persons entrusted with secure access and/or those whom have been assigned a specific role in relation to an ERDS, shall be subject to a state and federal level criminal record check through fingerprinting. The intent of this section is to identify those convictions that would disqualify an individual from obtaining approval to perform in a role requiring fingerprinting. In addition, as established in section 11105 of the Penal Code, the ERDS Program shall request subsequent arrest notification. The section is necessary so that the responsibilities of both an applicant requesting a fingerprint background check and the ERDS Program are understood.

**§ 401 Role Based Fingerprinting Requirement**

Because access to an ERDS shall be dependent on a role granted to an individual, this section is necessary to identify the roles assigned that shall require an individual to meet the fingerprinting requirements. In addition, this section outlines the responsibilities of an applicant requesting fingerprinting, of the County Recorder and of the ERDS Program, ensuring compliance with these regulations.

## Article 5. Baseline Requirements and Technology Standards

**§ 500 Basis for the Baseline Technology and Requirements Standards.**

In relationship to the development of an ERDS and to ensure that the intent of the ERDA is being addressed, this section defines the areas of availability, integrity and confidentiality. All of these components, combined, shall meet the requirements of establishing minimum standards and guidelines, based on industry "best practices".

**§ 501 Standards and Guidelines.**

This section stipulates the resources used to set the standards and guidelines for establishing the minimum requirements for the security of an ERDS. In addition, this section requires that an operational ERDS conforms within 2 years to any update, revision or replacement of a standard or guideline. The purpose of stating this requirement is to ensure that the integrity of information being transferred electronically is being maintained at the highest level of security, meeting the requirements of the ERDA.

**§ 502 Instrument Type.**

This section makes clear the two types of instruments, or types of documents, that may be delivered and returned as a digital or digitized electronic record. With each type of instrument being processed come requirements which are stated here. Within the regulations, these instruments shall be referred to as Type 1 and Type 2.

**§ 503 Operating Procedures.**

The responsibility shall lie with the County Recorder establishing an ERDS to develop ERDS operating procedures. The established operating procedures shall be subject to audit. This section outlines what the procedures shall

contain to be acceptable by the Department of Justice (DOJ) and a DOJ approved Computer Security Auditor.

**§ 504 System Implementation.**

Depending on the needs of a County Recorder and the various types of documents that will be processed electronically, a determination by the County Recorder as to what type of system shall be implemented will be made based on the specifications outlined in this section.

**§ 505 Payload Structure, Content and Usage.**

The information being delivered and/or returned is referred to in these regulations as the payload. Each ERDS shall contain a payload structure. Although, through a contract with an Authorized Submitter, there may be additional requirements, this section outlines, at a minimum, what is required by any ERDS delivering and/or returning a payload and describes the content and allowable usage.

**§ 506 Uniform Index Information.**

AB 578 requires that all digital electronic records and digitized electronic records being transmitted through ERDS be capable of uniform indexing. It shall be at the County Recorders discretion as to the content of uniform index information.

**§ 507 Electronic Signature of a Notary.**

When a signature is a required to be accompanied by a notary's seal or stamp, an ERDS payload shall be capable of including that information. This section outlines the requirements of an ERDS that shall include the information about the electronic signature of a notary.

**§ 508 Security Requirements for Data Integrity.**

The purpose of these regulations is to ensure the integrity of the data being transmitted via an ERDS. This section outlines the action to be taken when contamination is detected for either Type 1 or Type 2 instruments.

**§ 509 Security Requirements for Payload Protection.**

Payloads being both transmitted and stored shall employ encryption to protect confidentiality until it is decrypted by the intended recipient. Once decrypted, the responsibility of the content is that of the intended recipient. This section describes the protections measures to be taken for the payload of both Type 1 and Type 2 instruments during transmission and storage.

**§ 510 Security Requirements for Computer Workstations.**

This section outlines the minimum security requirements for ERDS computer workstations used to submit and/or return ERDS payloads. This section is included to ensure that the County Recorder understands his/her responsibility to ensure the security requirement is enforced.

**§ 511 Security Requirements for Computer Media.**

To ensure the confidentiality and security of the ERDS, the DOJ chose an industry "best practice" methodology of establishing layered security standards that protect the ERDS payload from the beginning of the process to the end of the process. This is achieved by defining the minimum baseline security requirements for an ERDS System. The end of the process is typically when data is written to other types of media for off site storage, disaster recovery or archiving or when older equipment is replaced. This section describes the steps that must be taken to maintain the security and confidentiality of the ERDS when storing on storage media, or reallocating ERDS hardware or storage media for other purposes.

**§ 512 ERDS Identification Security Requirements.**

To ensure the confidentiality and security of the ERDS the DOJ chose an industry "best practice" standard or process for establishing confidence in remote user identities electronically presented to the ERDS. DOJ uses a multi-factor authentication process to protect the security and confidentiality of the ERDS. This multi-factor approach is designed to prevent threats such as eavesdropper, replay, on-line guessing, verifier impersonation, and man-in-the middle attack. To achieve this level of security any individual with secure access to the ERDS must be enrolled and undergo an identity proofing process in which their identity is bound to a credential or certificate. Thereafter, the individual is remotely authenticated to the ERDS system over the network using their credential or certificate in an authentication protocol. This section provides the requirements for identification security.

**§ 513 ERDS Authentication Security Requirements.**

The multi-factor authentication process, chosen by DOJ to protect the integrity, availability and confidentiality of the ERDS, requires an individual with ERDS secure access to be enrolled with their identity bound to a credential or certificate. The ERDS authenticates the credential or certificate based on proof of possession of a cryptographic key by the individual attempting to access the ERDS using a cryptographic authentication protocol. The cryptographic authentication protocol allows an individual to demonstrate to a verifier that he or she has or knows the secret certificate or credential, in a

manner that protects the secret from compromise by different kinds of attacks. Cryptography assists with meeting the ERDS security objective of availability because it prevents accidental, while assuring that service is not denied to authorized individuals. This section provides the cryptographic and password standard that must be used when developing an ERDS and is based on industry "best practices".

**§ 514 ERDS Role Based Security Requirements.**

Access to an ERDS shall be role based and the responsibility of the County Recorder to assign those roles. This section outlines the security requirements to be met by users for both Type 1 and Type 2 instruments.

**§ 515 ERDS Server Security Requirements.**

The multi-factor authentication process chosen by DOJ to protect the integrity, availability and confidentiality of the ERDS requires an individual with ERDS secure access to be enrolled with their identity bound to a credential or certificate. The ERDS authenticates the credential or certificate based on proof of possession of a cryptographic key by the individual attempting to access the ERDS using a cryptographic protocol. In a multi-layered security approach it is also important where this authentication occurs. The ERDS technical design requires the authentication to occur on a server that is isolated from other organizational functions that would expose the ERDS to unnecessary security vulnerabilities. The design also requires that the authentication occur on a proxy server. Using a proxy server prevents an unauthorized individual from reaching the server used to process or store ERDS transactions. Again security is a layered process with checks and balances at a number of points all of which are intended to meet the security goal of enabling the County Recorders to meet their mission/business objectives by enabling the ERDS with due care consideration of Information Technology related risks to the Recorder, its partners and customers. This section provides the minimum server standards or requirements that must be used when developing a secure access ERDS and is based on industry "best practices".

**§ 516 ERDS Security Requirements for Network Security.**

The multi-factor authentication process chosen by DOJ to protect the integrity, availability and confidentiality of the ERDS, requires an individual with ERDS secure access to be enrolled with their identity bound to a credential or certificate. The ERDS authenticates the credential or certificate based on proof of possession of a cryptographic key by the individual attempting to access the ERDS using a cryptographic protocol. It is also important where this authentication occurs. The ERDS technical design requires the authentication to occur on a server that is isolated from other

organizational functions that would expose the ERDS to unnecessary security vulnerabilities. The design also requires that the authentication occur on a proxy server. The technical design is also specific about the requirements for network security. The integrity and confidentiality of ERDS information during transmission over a communication network can only be assured if good Information Technology practices for network security are used. Without them the ERDS would be vulnerable to network sniffing, spoofing, service denial attacks, or a number of other known hacker techniques for gaining access to a system through a vulnerable network design. This section provides the minimum network security standards or requirements that must be used when developing a secure access ERDS and is based on industry "best practices".

**§ 517 Physical Security.**

To prevent unauthorized access or use of an ERDS server, the County Recorder shall establish operating procedures. This section outlines the minimum requirements to an ERDS operating procedures and/or agreements established by a County Recorder.

**§ 518 Auditable Events, Incidents and Reporting.**

To maintain and regulate an ERDS functionality, an ERDS shall be subject to audits. Auditable events, as described within these regulations shall be logged for the purposes of audit, local inspection and review.

**§ 519 Proprietary Software.**

A DOJ approved Computer Security Auditor may not conduct a review of a Vendor's proprietary software, unless that software has affected the safety and security of an ERDS. This section is included to protect a Vendors interest in their software that has been provided through contract with a County Recorder for the development of an ERDS. In addition, the requirements of the County Recorder, a Vendor of ERDS software and a DOJ approved Computer Security Auditor are outlined to ensure the confidentiality security objective has been satisfied as stated within section 500 of this article.

**§ 520 Escrow Requirements.**

As required by AB 578, this section outlines information that shall be placed within an approved escrow facility for all ERDS.

**§ 521 Deposit of Software Modification into Escrow.**

When a change is made that affects the functionality of an ERDS, it is considered a substantive modification and shall require an update to source

code materials already being stored in an approved escrow facility. This section states that requirement.

**§ 522 Letter of Deposit.**

All information placed in an approved escrow facility by a developer or Vendor of ERDS Software shall notify all affected County Recorders by providing a Letter of Deposit. This section outlines the content of the Letter of Deposit.

**§ 523 Integrity of Materials.**

The intent of this section is to make it clear that access to the ERDS source code material, by the escrow representative, is necessary in order to determine that the escrow obligation of submitting a copy of the compiler needed to compile the ERDS source code, instructions for installation and use of the ERDS source code compiler, and instructions that facilitate reviews, modification and/or recompiling the source code by the ERDS Vendor has been met and is being maintained.

**§ 524 Retention and Disposition of Materials.**

The multi-layered security approach chosen to assure the availability, integrity and confidentiality of the ERDS extends to the retention and disposition of source code materials in escrow. Information stored at the Escrow facility provides technical detail that could be used to infiltrate the ERDS and as such must be protected in order to maintain the security of the ERDS. During the duration of the ERDS contract, the source code materials are subject to review and audit by a DOJ approved Computer Security Auditor. This section defines the requirements for the retention of ERDS source code materials for the term of the escrow agreement and that the escrow agreement shall provide for the disposition of source code materials in the event the escrow agreement terminates.

**§ 525 Access to Materials.**

Access to the ERDS source code material is necessary for the DOJ approved Computer Security Auditor to verify that a copy of all source code that implements ERDS functionality, a copy of the compiler needed to compile the ERDS source code, instructions for installation and use of the ERDS source code compiler, and instructions that facilitate reviews, modification and/or recompiling the Source Code, has been placed in the approved escrow facility. This section makes it clear that the Escrow agreement entered into by the developer and County Recorder shall allow for access to ERDS source code materials by a DOJ approved Computer Security Auditor hired for the purpose of conducting a computer security audit.

**§ 526 State Non-Responsibility.**

The requirement to place source code material into an approved escrow facility is to protect the County Recorders investment and is a common practice when the development of an application is outsourced. Any fees or liability associated with establishing an escrow contract is the cost of doing business and is not the responsibility of the Attorney General or the State of California as the choice to implement an ERDS is not a state mandate. This section is to make it clear that this is not the responsibility of the Attorney General or the State of California.

## Article 6. ERDS Certification

**§ 600 Establishing an ERDS.**

A County Recorder choosing to establish an ERDS must meet certain criteria and agree to specified responsibilities. It is important for a County Recorder to understand this regulation so that they understand what is required of them in order to establish an ERDS. This section outlines what is required and expected of the County Recorder to meet these requirements.

**§ 601 Certification Application Procedure.**

A county initially establishing an ERDS has the option of applying for certification of a Single-County operation or a Multi-County operation. A County Recorder of a Single-County operation shall be responsible for that particular county. A County Recorder of a Multi-County operation shall be either the Lead County Recorder of all participating counties or a Sub-County Recorder of a county participating in a Multi-County operation. Each scenario requires a County Recorder to apply for certification to establish an ERDS. It is necessary to go through the application process to regulate a county's operation and guarantee that a County Recorder understands their responsibility. This section outlines the requirements and process for the submission of an Application for Certification for each operation.

**§ 602 Substantive Modification Application Procedure.**

As defined in these regulations, a substantive modification is a change that affects the functionality of an established ERDS. When such a change occurs it shall be necessary for County Recorder to apply for an approval of the modification before initiating a change. All affected areas of the system, previously approved and certified, shall be considered invalid until the

modifications made have been approved through a security audit. This regulation is necessary to ensure the security of a certified system.

**§ 603 Non-substantive Modification.**

Because a non-substantive modification does not affect the functionality of an established ERDS, there shall be no need for a County Recorder to apply for approval of the modification and it shall not require a security audit. The documenting of non-substantive modifications is the responsibility of the County Recorder and maintained information shall be subject to review to ensure the proper maintenance of an ERDS.

**§ 604 Approval of Application.**

An approval letter and the issuance of a System Certification of Operation shall be issued by the ERDS Program upon approval of an Application for System Certification or Approval of a Substantive Modification. The issuance of these certifications will ensure that all processes, requirements and procedures as outlined in these regulations are being met and that an ERDS is operating as a secure system.

**§ 605 Incomplete Application.**

This section identifies what could cause an Application for System Certification or Substantive Modification to be returned to a County Recorder. The ERDS Program will inform a County Recorder in writing and allow 90 days for the applicant to respond. These guidelines are needed to prevent pending an application for an extended period of time. If no response is received the application will be denied. Because of the voluntary nature of this program, a denial does not prevent a county from submitting again at a later date.

**§ 606 Denial of Application.**

AB 578 allows for a certification to be withdrawn for good cause. This section defines good cause and establishes that a County Recorder will receive written notification explaining the reason for denial. A denial does not prevent a county from submitting again at a later date.

**§ 607 Change of County Recorder.**

In the event a County Recorder changes after an ERDS has been implemented, notification to the ERDS Program is to be made within 30 days. This section requires the new County Recorder to sign a Statement of Understanding which will act as notification to the ERDS Program that the

newly appointed County Recorder is aware of his/her responsibilities. This is needed to ensure that the operation of an ERDS is not jeopardized due to an uninformed County Recorder during the transition.

**§ 608 Change of physical and/or mailing address and/or contact information for a County Recorder.**

This section requires a County Recorder to notify the ERDS Program of any change to the mailing address or contact information. The most current information is needed to maintain updated records within the ERDS Program for the continued oversight of an ERDS as required by AB 578.

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

As required by AB 578, a County Recorder shall be responsible for maintaining a list of all individuals and the role they have been granted in association to an ERDS. The list is subject to review during audits and local inspections. When changes occur to that listing, the County Recorder is required to notify the ERDS Program. By notification the County Recorder and the ERDS Program are able to verify that an ERDS is not being accessed by unauthorized individuals.

**§ 610 Expiration of Certification.**

This section establishes that under normal operation an ERDS certification shall remain in effect without the need for renewal. However, if a certification has been suspended by the ERDS Program or if a County Recorder withdraws their participation, an ERDS certification shall be invalid and would require a County Recorder to repeat the certification process.

**§ 611 Withdrawal of Certification.**

A County Recorder may choose to withdraw an ERDS certification. In order to cease operation it shall be the County Recorders responsibility to initiate the withdrawal. Withdrawing an ERDS certification does not prevent a County Recorder from participating at a later date. This section outlines the requirements for withdrawing and stipulates that once withdrawn, a County Recorder shall proceed with the initial steps for System Certification if they wish to participate in the ERDS in the future.

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

A replacement certificate or copies of documents pertaining to an application submission shall be provided by the ERDS Program at the request of a County Recorder or his/her designee. To protect the confidentiality of information

contained in an application and to assure that a replacement certificate is needed, the County Recorder or his/her designee shall submit a fee and a form specifically for that purpose, signed and dated under penalty of perjury that the request is necessary.

## Article 7. Computer Security Auditor Approval

### § 700 DOJ Computer Security Auditor Application Procedure.

As required by AB 578, criteria listed in this section clearly state the requirements of a computer security auditor seeking approval of the Attorney General to become a DOJ approved Computer Security Auditor. Complying with the requirements of this section shall insure that the individual meets all criteria and possesses the significant experience required to conduct a thorough audit of an ERDS and that the security of the system shall not be jeopardized.

### § 701 Approval of Application.

An Approval Letter and ERDS Certificate of Approval shall be issued to the DOJ approved Computer Security Auditor. In addition, the name of the individual shall be posted to the ERDS web page. There, a County Recorder shall find the listing of all DOJ approved Computer Security Auditors and shall choose one to contract with to perform security testing as required by AB 578. The approval issued and the posting of the individuals name to the ERDS web page verifies that the individual is qualified to provide the security testing required ensuring the security of the ERDS.

### § 702 Incomplete Application.

This section identifies what could cause an Application for Computer Security Auditor Approval to be returned to the applicant. The ERDS Program will inform the applicant in writing and allow 90 days for the applicant to respond. If no response is received the application will be denied. Because of the voluntary nature of this program, a denial does not prevent an individual from submitting again at a later date. As required by AB 578, a request for Computer Security Audit Approval shall be completed within 90 days. These guidelines are needed to prevent pending an application for an extended period of time. In addition, it is necessary to ensure that an applicant clearly understands that a complete application, all supporting documentation and required fees are to be submitted together. Failure to do so shall result in all submitted documentation being returned.

**§ 703 Denial of Application.**

An application not satisfying the requirements for Computer Security Auditor Approval may be denied for good cause. An applicant shall receive written explanation for a denial and the application returned. A denial does not prevent an individual from submitting at a later date. As required by this Article certain experience standards shall be met, and if not, the applicant would be considered inexperienced in relation to these regulations. A denial is necessary to protect the security of an ERDS, a County Recorder and public interest.

**§ 704 Expiration of Approval.**

A DOJ Computer Security Auditor Approval shall be valid for 3 years from the date of issuance of the certificate of approval unless suspended or the individual withdraws their request for approval. The 3 year period has been established to ensure that all application criteria remain current.

**§ 705 Renewal of Approval.**

The responsibility to renew shall be that of the certificate holder. An approval shall be renewed prior to the expiration date in order to remain valid. If an application for renewal is received after the expiration date, it shall be returned with instruction to proceed with the initial approval process. The necessity for a renewal is that the ERDS Program is assured that the individual has maintained a qualified status and continues to meet the security requirements and qualifications as outlined in this Article.

**§ 706 Withdrawal of Approval**

A DOJ approved Computer Security Auditor may choose to withdraw their certificate by submitting an Application for Withdrawal. The application shall note the date that services are considered invalid. The ERDS Program shall provide written verification of receipt of the request and inform the applicant that their name has been removed from the ERDS Approved Security Auditor listing. Withdrawing does not prevent a Computer Security Auditor from requesting approval in the future. To ensure that a County Recorder is contracting with a DOJ approved Computer Security Auditor, this process is essential to enable the ERDS Program to remove any Computer Security Auditors withdrawing their approval from the ERDS listing.

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

A replacement certificate or copies of documents pertaining to an application submission shall be provided by the ERDS Program at the request of a DOJ approved Computer Security Auditor. To protect the confidentiality of

information contained in an application and to assure that a replacement certificate is needed the DOJ approved Computer Security Auditor shall submit a fee and a form specifically for that purpose, signed and dated under penalty of perjury that the request is necessary.

## Article 8. Vendor of ERDS Software Certification

### § 800 Certification Application Procedure.

As required by AB 578, the Attorney General is required to establish procedures for the initial certification of vendors offering software and other services. This section clearly states the requirements to be met by an individual applying for certification as a Vendor of ERDS Software and shall be done prior to contracting with a County Recorder. In addition to a completed application, proof of a fingerprint background check and submission of required fees, an applicant shall provide reference or service agreement information including specific details as outlined. The information submitted insures that the applicant is qualified to meet the established requirements for the development of ERDS Software.

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

After entering into a contract with a County Recorder, a Certified Vendor of ERDS Software may require additional vendor employees or vendor contract employees for the development of an ERDS. All employees of the vendor shall be subject to a fingerprint background check and proof of that fingerprinting shall be provided to the County Recorder. To meet the requirement of AB 578, maintaining a list of employment positions or classifications, the County Recorder shall be responsible for notifying the ERDS program of receiving proof of fingerprinting on those individuals and maintaining the list of those employees and their roles. The list shall be subject to audit and local inspection. This regulation is necessary to ensure that those individuals associated with the development of the ERDS are not disqualified. In the event of a subsequent arrest or should an employee leave service, the list assists the County Recorder in notifying the ERDS Program that they are no longer interested in that individual.

### § 802 Approval of Application.

An Approval Letter and a Vendor of ERDS Software Certificate shall be issued to the individual upon determining that requirements and qualifications have been satisfied. The issuance of the Certificate is verification that a vendor has completed the certification process and is qualified to enter into a contract with a County Recorder as a Vendor of ERDS Software.

**§ 803 Incomplete Application.**

This section identifies what could cause an application for a Vendor of ERDS Software to be returned. The ERDS Program will inform an applicant, in writing, of an incomplete application and allow 90 days for the applicant to respond. If no response is received, the application will be denied. Because of the voluntary nature of this program, a denial does not prevent an individual from submitting again at a later date. This regulation is necessary to ensure that an applicant clearly understands that a complete application, all supporting documentation and required fees are to be submitted together. Failure to do so shall result in all submitted documentation being returned.

**§ 804 Denial of Application.**

An application not satisfying the requirements for a Vendor of ERDS Software may be denied for good cause. An applicant shall receive written explanation for a denial and the application returned. A denial does not prevent an individual from submitting at a later date. As required by this Article, certain experience standards and system requirements shall be met, and if not, the applicant would be considered inexperienced in relation to these regulations. A denial is necessary to protect the security of an ERDS, a County Recorder and public interest.

**§ 805 Expiration of Certification.**

A certification for a Vendor of ERDS Software shall be valid for 3 years from the date of issuance of the certificate unless suspended or the individual withdraws their request for approval. The 3 year period has been established to ensure that all application criteria remain current.

**§ 806 Renewal of Certification.**

The responsibility to renew shall be that of the certificate holder. An approval shall be renewed prior to the expiration date in order to remain valid. If an application for renewal is received after the expiration date, it shall be returned with instruction to proceed with the initial approval process. The necessity for a renewal is that the ERDS Program is assured that the individual has maintained a qualified status and continues to meet the security requirements and qualifications as outlined in this Article.

**§ 807 Withdrawal of Certification.**

A Vendor of ERDS Software may choose to withdraw their certificate by submitting an Application for Withdrawal. The application shall note the date that services are considered invalid. The ERDS Program shall provide written

verification of receipt of the request and inform the applicant that their certificate is no longer valid. Withdrawing from certification does not prevent a Vendor of ERDS Software from requesting approval in the future. This process is essential to ensure that a County Recorder is contracting with a vendor who has met all requirements of this Article to be a Certified Vendor of ERDS Software.

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

A replacement certificate or copies of documents pertaining to an application submission shall be provided by the ERDS Program at the request of a Certified Vendor of ERDS Software. To protect the confidentiality of information contained in an application and to assure that a replacement certificate is needed, the Certified Vendor of ERDS Software shall submit a fee and a form specifically for that purpose, signed and dated under penalty of perjury that the request is necessary.

## Article 9. Audits and Oversight

### § 900 Security Audits.

The different types of audits to be performed are as follows:

- Initial System Audit –Audit of entire system conducted initially; required for certification.
- Biennial Audit – Audit conducted by a DOJ approved Computer Security Auditor in alternating years of the local inspection. This audit is a full system audit that shall be performed in the production and operational environment.
- Modified System Audit – Audit required as a result of a request for Substantive Modification to an existing certified Single-County or a Multi-County ERDS. This audit shall only pertain to the components of a system that have been modified and shall be conducted by a DOJ approved Computer Security Auditor. A successful Modified System Audit does not replace the Biennial Audit.
- Modified System Incident Audit – Audit required as a result of a reported incident that compromises the safety and security of an ERDS. This audit shall only pertain to only the components of a system that were found to have been compromised and shall be conducted by a DOJ approved Computer Security Auditor.
- Local Inspection – Audit conducted by ERDS Program staff in alternating years of the Biennial Audit. This audit provides oversight and regulation of non-technical processes to ensure that responsibilities of those associated with an ERDS are being met.

As required by AB 578, the Attorney General shall be responsible for the oversight and regulation of an ERDS. This requirement shall be met by conducting a series of audits and local inspections at various times established within these regulations. These audits are necessary to ensure a certified system is safe and secure from vulnerabilities, that operating procedures are in place, and that public record can not have information inserted or deleted, or be modified and/or manipulated in any manner. All audit results shall be provided to the County Recorder responsible for the system being audited and shall include documentation that addresses the status of all auditable areas as listed within this section.

**§ 901 Audit Report Format.**

This section specifically describes the format and identifies the information that shall be included in an Audit Report. This regulation is necessary to ensure that all areas of a system audit have been addressed by the DOJ approved Computer Security Auditor and that all findings and recommendations have been clearly identified and noted. By maintaining a uniform account of each audit, the responsibility of the Attorney General to provide oversight and regulation shall be met by monitoring the safety and security of ERDS.

**§ 902 Local Inspection.**

An ERDS Program representative shall conduct a local inspection of counties operating and/or associated with a certified ERDS. It shall be conducted in alternating years of the biennial audit. The purpose of this section outlines the details of the local inspection. The ERDS Program representative provides oversight of the associated processes of an operating ERDS. The County Recorder or his/her designee shall provide all records, including auditable logs, reported incident documentation, DOJ approved Computer Security Auditor reports, certification documentation for themselves and associated counties, if any, logs of all individuals assigned a role requiring fingerprinting, copies of certificates and contracts of DOJ approved Computer Security Auditors and Vendors of ERDS Software to the ERDS Program Representative for their review. Once completed, the ERDS Program Representative shall provide inspection results to the County Recorder or his/her designee. The ERDS Representative shall work with the County Recorder to resolve any non-compliance issue(s). If a County Recorder fails to correct an issue, the ERDS Program shall issue a letter of ERDS suspension.

These measures are necessary for the ERDS program to provide regulation and ongoing oversight of the administrative processes and to ensure all those

individuals involved understand their responsibility in maintaining a secure environment for an operating ERDS.

**§ 903 Incident Reporting.**

As required by AB 578, a County Recorder, a DOJ approved Computer Security Auditor, District Attorney or Attorney General discovering or suspecting security violations or discovering that a system is vulnerable to fraud or intrusion, shall be responsible for immediately reporting the incident to the ERDS Program, DOJ approved Computer Security Auditor, District Attorney, and the county's Board of Supervisor. This section outlines the processes and responsibilities to follow, should an incident occur. This regulation is necessary to guard the safety and security of an ERDS. All written documentation regarding any incident shall be maintained for statistical purposes. The information will be required in an evaluation report to the Legislature on or before June 30, 2009, as stated in AB 578.

**§ 904 Suspension and Termination of Certification.**

For the purpose of these regulations, the terms "suspend" and "terminate" are considered interchangeable and are used to designate removal of all privileges to an ERDS operation. This section outlines the reasons for the suspension or termination of a certified ERDS. Non-compliance of any of the areas identified shall result in the ERDS program enforcing this regulation. By establishing these guidelines, the Attorney General satisfies the requirement of providing regulation and oversight and ensuring the safety and security of an ERDS.

**§ 905 Notification.**

The ERDS Program shall notify a County Recorder, by certified mail, that a certification of an ERDS has been terminated or suspended as a result of any reason constituting such action. Copies shall be sent to the Board of Supervisors, the Attorney General and the District Attorney. This regulation is necessary to inform a non-compliant county of the need to stop all ERDS functions immediately and that their authority to operate an ERDS has been removed. This regulation provides the continual regulation and oversight by the Attorney General as required by AB 578.

**§ 906 Reconsideration.**

This regulation makes available, to the County Recorder, the option to submit a written request to the ERDS program asking for reconsideration of an ordered terminated or suspended ERDS. In cases where an ERDS operation was terminated or suspended due to the discovery of vulnerabilities, a Modified System Incident Audit shall be required before resuming an ERDS

operation. Included in this section are Administrative reasons why an ERDS operation can be terminated or suspended. In such cases, taking corrective action shall result in the reinstatement of operation. This section is needed to maintain the security of ERDS operations by allowing the ERDS program to enforce these regulations, therefore meeting the responsibility of oversight by the Attorney General.

ATTACHMENT 1
ECONOMIC IMPACT STATEMENT

A. Estimated Private Sector Cost Impacts

2. The total number of businesses impacted: Unknown, participation is voluntary.

C. Estimated Benefits

1. Benefits that may result from these regulations and who will benefit:

The types of businesses impacted: The types of private sector businesses that could be impacted consist of those businesses associated with real estate transactions in preparation for recording documents with a County Recorder. Such industry entities may include Title Companies, Banks, Mortgage Companies, etc. In addition, vendors of system and software development as well as industry entities representing information systems security could be impacted if in agreement with a participating County Recorder's electronic recording delivery system. These regulations allow for the implementation of technologies that will result in significant net savings to participants. Businesses will be employed to implement the technologies.

ATTACHMENT 2
FISCAL IMPACT STATEMENT

A. Fiscal Effect on Local Government

2. Additional expenditures of approximately $ Unknown in the current State Fiscal Year which are not reimbursable by the State pursuant to Section 6 of Article XIII B of the California Constitution and Sections 17500 et seq. of the Government code because this regulation:

e. Will be fully financed from the following:

- A County Recorder may impose a fee in an amount up to and including one dollar ($1) for each instrument that is recorded by the county.
- A County Recorder may impose a fee upon any vendor seeking approval of software and other services as part of an ERDS.
- A County Recorder may impose a fee upon any person seeking to contract as an authorized submitter.

Authorized by Section 27397 (c)(1), (2), (3)

Note: These regulations could result in additional costs to local government to the extent that they choose to participate in the program. These costs would not be reimbursable by the state because participation in the program is optional.

B. Fiscal Effect on State Government

1. Additional expenditures of approximately $ 648,182.00 in the current State Fiscal Year.

Note: Pursuant to Government Code section 27397(a) and (d), any State costs would be reimbursed by local governments that choose to participate in the program. Therefore, this program would not result in any new General Fund costs to the state.

See Attachment 3 for projected calculations and assumptions of fiscal impact for the current year and two subsequent Fiscal Years.

ATTACHMENT 3
PROJECTED CALCULATIONS AND ASSUMPTIONS
CURRENT YEAR AND TWO SUBSEQUENT YEARS

The method of calculating a counties proportionate share of the cost per year to participate in electronic recording is outlined in Article 3, section 301 of these regulations. The calculations and assumptions within this attachment are estimated.

| **Projected Fiscal Detail Expenditures** | **FY 06/07** | **FY 07/08** | **FY 08/09** |
|---|---|---|---|
| **Personal Services** | | | |
| Salaries | $317,842 | $324,326 | $327,442 |
| Staff Benefits | $127,920 | $130,679 | $132,040 |
| **Total Personal Services** | **$445,762** | **$455,005** | **$459,482** |
| **Operating Expenses & Equipment** | | | |
| General Expense | $ 15,655 | $ 15,655 | $ 15,655 |
| Printing | $ 6,720 | $ 6,720 | $ 6,720 |
| Communications | $ 10,950 | $ 10,950 | $ 10,950 |
| Postage | $ 3,500 | $ 3,500 | $ 3,500 |
| Travel-In-State | $ 15,000 | $ 15,000 | $ 15,000 |
| Travel Out-Of-State | $ 5,000 | $ 5,000 | $ 5,000 |
| Training | $ 8,950 | $ 8,950 | $ 8,950 |
| Consultant Prof Serv – External | $ 43,719 | $ | $ |
| Data Processing | $ 15,500 | $ 15,500 | $ 15,500 |
| Equipment | $ 7,000 | $ 7,000 | $ 7,000 |
| Other Items of Expense | $ 10,000 | $ 10,000 | $ 10,000 |
| **Total Operating OE & E** | **$141,994** | **$ 98,275** | **$ 98,275** |
| **Total Direct Excess Spending Authority Departmental Services** | **$587,756** | **$553,280** | **$557,757** |
| **TOTAL** | **$587,756** | **$553,280** | **$557,757** |