Electronic Recording Delivery System
Baseline Requirements &Technology Standards Handbook

Addendum to the following ERDS Handbooks:
Vendor of ERDS Software Certification
Computer Security Auditor
System Certification

Office of the Attorney General
California Department of Justice

November 2016

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 INTRODUCTION

The purpose of this document is to establish the minimum baseline technological guidelines, requirements, procedures, and standards in the areas of security, reliability, and uniformity following the enactment of the Electronic Recording Delivery Act (ERDA) of 2004, to establish an Electronic Recording Delivery System (ERDS) as provided for in the California Code of Regulations (CCR), Title 11, Division 1, Chapter 18, Articles 1 through 9. As such, this document uses technical terms to describe information technology and is intended for Computer Security Auditors, Vendors of ERDS Software, and individuals having technical responsibilities for an ERDS. This document does not, however, specify design details that may be necessary to fully implement an ERDS meeting the intent of the ERDA. While this document includes requirements for the security, audit, and escrow of an ERDS, it should be referenced in conjunction with the ERDS handbooks pertaining to the Vendor of ERDS Software, Computer Security Auditor, and System Certification.

1.1 OVERVIEW

A County Recorder may, in lieu of written paper, accept for recording digital electronic records and digitized electronic records, subject to specified conditions. The ERDS Program has established baseline technological and procedural specifications that detail the conditions for delivering, and, when applicable, returning digital electronic records and digitized electronic records. Nothing in these specifications shall be construed to administer any of the processes or procedures relating to the business of a County Recorder of the State of California. Specifications established by the ERDS Program are intended to assure that the ERDS is secure and that ERDS operating procedures are sufficient to assure the continuing security and lawful operation of the ERDS. Additionally, these specifications do not address prevention for any tampering or fraudulent documents prior to transmitting via an ERDS.

1.1.1 Focus of Security

An ERDS is a system to deliver for recording, and, when applicable, return to the party requesting recording, digitized or digital electronic records. Considering the requirements for security and the openness of the Internet, each ERDS shall focus on protecting the confidentiality and integrity of digital electronic records and digitized electronic records during the process of transmission and storage using an ERDS. In addition to the delivery, and, when applicable, the return of digital electronic records or digitized electronic records, this document addresses the handling of uniform index information and information about the electronic signature of a notary.

1.1.2 Responsibilities of the County Recorder

The County Recorder shall be responsible for ensuring an ERDS meets the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. With respect to an ERDS, the County Recorder may delegate tasks to designees and representatives, assign responsibility by contract or agreement, and grant authority through policies and procedures; however, the overall safety and security of an ERDS shall remain the responsibility of the County Recorder. Where the term “County Recorder” is used in this document, the County Recorder shall determine the necessary resources and means to meet the requirement.

1.1.3 Statutory, Industry and Technical Terminology

These specifications do not limit the content or format of digital electronic records and/or digitized electronic records. Because the state of technology is such that digital electronic records and digitized electronic records are not reliably distinguishable by automated means, additional precautions shall be taken to meet the requirements of the Electronic Recording Delivery Act (ERDA) of 2004.

The ERDA refers to two types of instruments that may be delivered, and, when applicable, returned as digital electronic records and/or digitized electronic records. For the purposes of an ERDS, these instruments are categorized as "Type 1" and "Type 2". A "Type 1" instrument is defined to mean an instrument affecting a right, title, or interest in real property. A "Type 2" instrument is defined to mean an instrument of reconveyance, substitution of trustee, or assignment of deed of trust. The real estate industry refers to Type 1 and Type 2 instruments as "front-end" and "back-end" documents, respectively. Because these terms do not necessarily reflect the method of delivery (digital or digitized) or the characteristics of computer-generated files, the County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type to meet the requirements of the ERDA. A summary of the relationships among statutory, industry and technology terms is provided in Table 1 - Instrument Types.

1.1.4 Fiscal Impact

All ERDS shall be designated as Type 1 or Type 2 or Type 1 and 2 and whether a return function is included, when applicable. For each ERDS, the types of instruments and the characteristics of computer-generated files depend on the business requirements of the County Recorder. For this reason, the types of instruments submitted, and, when applicable, returned, as well as the characteristics of computer-generated files transmitted via an ERDS, are at the discretion of the County Recorder. If the County Recorder allows for the delivery of Type 1 and/or Type 2 instruments electronically, then the transmission of those instruments shall meet all of the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

To provide options in implementing an ERDS, several approaches are described in this document. Current information technologies offer a wide variety of approaches. For illustrative purposes, the approaches described in Section 1.2, Approaches, provide examples of architectures suitable for meeting the requirements of the ERDA. The examples are not intended to either specify or limit the design of, or technologies employed for, an ERDS. Rather, the examples are given to illustrate how technologies can be employed to meet the requirements of the ERDA while providing options that limit the fiscal impact on County Recorders.

1.1.5 Use of Vendors

A County Recorder may employ a Vendor of ERDS Software, use in-house resources, or enter into an agreement with another public entity in establishing an ERDS. Computer Security Auditors, Authorized Submitters, Agents, and Vendors of ERDS Software shall be separate entities. Authorized Submitters may employ a third-party vendor as an Agent provided that the third-party vendor is neither a Computer Security Auditor nor a Vendor of ERDS Software. (For further clarification, refer to the definitions for "Agent" and "Vendor of ERDS Software" contained in Section 7, Acronyms and Definitions.

1.2 APPROACHES

Ensuring the secure delivery and integrity of Type 1 and Type 2 instruments is achieved by using the minimum baseline security requirements as defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and outlined in Section 4.2, Minimum Security Requirements. Specific architectural details are ERDS-design dependent and may not be fully explained in this document. The selection of specific technical design approaches shall be at the discretion of the County Recorder.

Irrespective of the ERDS design, the minimum security requirements, as specified in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and outlined in Section 4.2, Minimum Security Requirements, shall be met by protecting the payload structure and content for both Type 1 and Type 2 instruments. All ERDS for either Type 1 or Type 2 payloads shall be protected by the use of encryption, both in transmission and storage, until decrypted by the intended recipient. Once decrypted by the intended recipient, the security of the contents shall become the responsibility of the intended recipient. The roles and responsibilities of ERDS participants, including, but not limited to, Agents and Vendors of ERDS Software, shall be consistent with Section 4.3.1.3, Authorization Requirements and Section 7, Acronyms and Definitions. While the ERDS Regulations allow flexibility in approach, the security and testing requirements shall be met.

1.2.1 Type 1 ERDS

This illustrative approach requires fingerprinting of each Authorized Submitter and offers robust security. Only those individuals granted permissions under the role of “Secure Access” (Refer to Section 4.3.1, Access Control) shall be permitted access to a Type 1 ERDS. Type 1 instruments shall be submitted as digitized electronic records. One or more servers are employed to guide an Authorized Submitter through ERDS processes and store the ERDS payloads.

Confidentiality, integrity and authenticity are preserved by encrypting and “signing” a data structure called the “ERDS payload”. Data confidentiality is preserved by encrypting the ERDS payload. Data integrity and authenticity are preserved by “signing” the ERDS payload. Delivery occurs via commonly available secure transfer protocols, such as Transport Layer Security (TLS) or a Virtual Private Network (VPN) to a Type 1 ERDS.

The identity of each Authorized Submitter and County Recorder Designee who accesses the Type 1 ERDS is verified using two factors: (1) a user ID and password, and (2) a digital certificate validated by a certificate authority employing public key cryptography methods. The actual contents of Type 1 ERDS payloads shall be verified to ensure adherence to restrictions of instrument type.

1.2.2 Type 2 ERDS

This illustrative approach does not require the fingerprinting of an Authorized Submitter and makes the most use of existing information technology. In this approach, the transport mechanism is electronic mail; however, only Type 2 instruments shall be submitted by individuals granted permissions under the role of “Authorized Access”. (Refer to Section 4.3.1, Access Control)

Confidentiality, integrity and authenticity are preserved by encrypting and “signing” e-mail. Data confidentiality is preserved by encrypting an attachment to an electronic mail message. Data integrity is preserved by “signing” the attachment. The attachment is a data structure called the “ERDS payload”. (Refer to Section 2, Data Architecture.) Authenticity is preserved by “signing”

the electronic mail message itself. Delivery occurs via commonly available electronic mail transfer protocols, such as the Simple Mail Transfer Protocol (SMTP).

The identity of each Authorized Submitter and County Recorder Designee, who sends a Type 2 ERDS payload, is verified using a digital certificate validated by a certificate authority employing public key cryptography methods. The actual contents of Type 2 ERDS payloads shall be verified to ensure adherence to restrictions of instrument type.

1.2.3 Type 1 and Type 2 ERDS

This illustrative approach requires fingerprinting of each Authorized Submitter with a role of "Secure Access", but not any Authorized Submitter with a role of "Authorized Access", and offers both robust security and separation of Type 1 instruments from Type 2 instruments. Individuals granted permissions under the role of "Secure Access", "Authorized Access", or "County Recorder Designee" (refer to Section 4.3.1, Access Control) shall be permitted access. One or more servers are employed to guide an Authorized Submitter through ERDS processes and store the ERDS payloads. The combination of a role-based access control system and an application server separates Type 1 instruments from Type 2 instruments.

Confidentiality, integrity, and authenticity are preserved and identity verified in the same manner as for Secure Access to a Type 1 ERDS.

An application server processes functions based on the role authorized in the role-based access control system. If an individual is granted permissions under the role of "Authorized Access", only Type 2 instruments may be submitted. If an individual is granted permissions under the role of "Secure Access", both Type 1 and Type 2 instruments may be submitted; however, Type 1 instruments shall be limited to digitized electronic records. In either case, the ERDS payloads are delivered to a Type 1 ERDS.

1.2.4 Content Inspections

Regardless of approach, the County Recorder shall make no assumptions about the content delivered via an ERDS. Until technology reliably distinguishes digital electronic records from digitized electronic records, the County Recorder shall have ERDS operating procedures that include inspection to determine that the content delivered via an ERDS meets the requirements of the ERDA. Specifically, if the County Recorder cannot assure, with 100 percent certainty, that the contents of a digital electronic record cannot be delivered as a digitized electronic record, and vice versa, and that a Type 1 instrument cannot be delivered as a Type 2 instrument, and vice versa, then the contents of all Type 1 and Type 2 instruments shall be inspected before being accepted.

1.3 THE ERDS BOUNDARY

This section describes the boundary of an ERDS. The boundary of an ERDS is defined to include that hardware, software, network connections and storage media specifically designed and/or designated for the delivery, and, when applicable, return of Type 1 and/or Type 2 instruments. Such hardware, software, storage media, and network connections shall be designated by the County Recorder establishing the ERDS and shall be included in system certifications, audits, local inspections, and reviews.

As such, hardware, software, storage media, and network connections not designated by the County Recorder shall:

1. Not be considered part of an ERDS.
2. Not be employed for the delivery of Type 1 or Type 2 instruments.
3. Not be included in system certifications, audits, local inspections or reviews.

1.3.1 Users

The ERDS shall support the ability of the County Recorder to grant access to any Authorized Submitter. The details of implementing processes such as establishing and deleting accounts, enabling encryption and decryption, and assigning roles are ERDS-design dependent and shall be implemented using resources at the discretion of the County Recorder.

Once granted access, an Authorized Submitter shall be able to submit Type 1 and/or Type 2 instruments depending on specific privileges granted by a County Recorder. An Authorized Submitter may be granted access to more than one ERDS; however, access to each ERDS shall remain under management control of the County Recorder establishing and responsible for the ERDS.

A County Recorder shall clearly define roles and responsibilities to ensure Type 1 and Type 2 instruments are correctly and securely submitted, delivered, and when applicable, returned to the intended recipients. Textual disclaimers or verbal disclaimers alone shall not be sufficient to control access to Type 1 and Type 2 instruments under the control of an ERDS.

1.3.2 Functionality

An ERDS is used by an Authorized Submitter to deliver Type 1 and/or Type 2 instruments to a County Recorder. An ERDS is also used by a County Recorder to return Type 1 and/or Type 2 instruments to an Authorized Submitter, when applicable. When Type 1 and Type 2 instruments are returned to an Authorized Submitter via an ERDS, the security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met. Any other responses or notifications transmitted via an ERDS shall not be required to meet the security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

When implemented, each ERDS may consist of hardware, software, storage media, and network connections that securely exchange messages and data.

A County Recorder may collaborate with another County Recorder and make use of a single ERDS. ERDS servers, if employed, shall be designated as “Single-County” or “Multi-County”. ERDS servers designated as Single-County shall be dedicated to serving a single county. ERDS servers designated as Multi-County shall serve more than one county as established by mutual agreement among County Recorders. Refer to the System Certification Handbook for procedures to apply for system certification of a Multi-County ERDS. Whether designated as a Single-County or Multi-County ERDS, all ERDS will be identified as either being Type 1, Type 2, or Type 1 and 2, and whether a return function is included, when applicable.

Servers employed for the purpose of implementing an ERDS may be dedicated to ERDS functions or integrated with other servers. Separate physical servers dedicated to performing an ERDS-server function are not required provided ERDS-server functions can be isolated from other server functions, as evidenced by audit. (Refer to Section 4.3.2, Server Security for more information.)

1.3.3 ERDS Implementation

In considering the characteristics of an ERDS and for illustrative purposes only, a conceptual ERDS boundary is depicted in Figure 1 - Conceptual ERDS Boundary. The components required to implement an ERDS may be installed and maintained on one or more servers designated for the purpose of implementing an ERDS. Components may be deployed to existing information technology in order to take advantage of available capabilities, but only if such deployment is necessary for the operation of an ERDS, and preserves the safety and security of the ERDS.

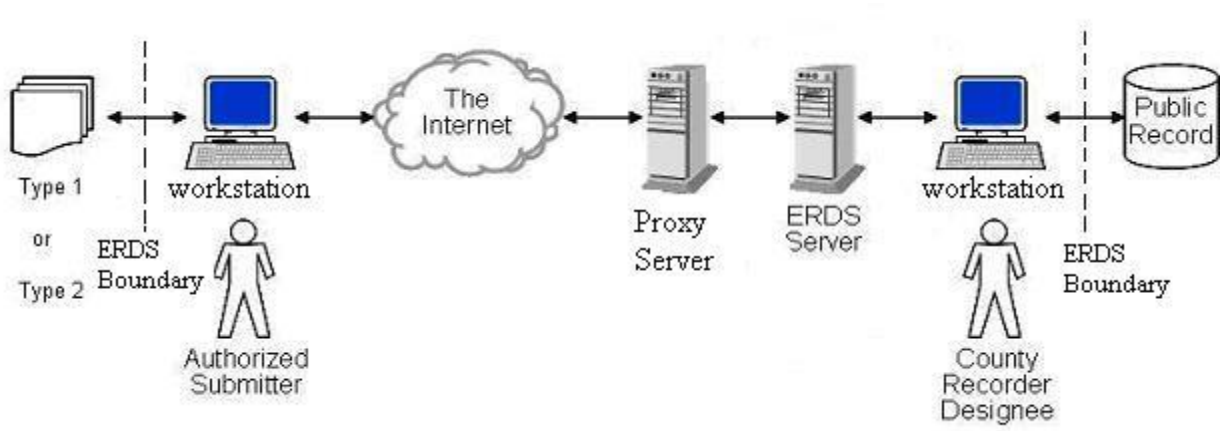

Figure 1 - Conceptual ERDS Boundary

For example, ERDS components may be deployed to a separate proxy server in order to take advantage of the ability to establish secure connections via the Internet and act as a proxy for an Authorized Submitter. As another example, an ERDS may take advantage of the existing network infrastructure of a County Recorder, provided the infrastructure is protected from unauthorized access. As a final example, the nature of web-based applications means at least some ERDS components may be deployed to workstations.

1.3.4 Approach Described in this Document

The specifications outlined in this document assume implementation of an ERDS operated via the Internet. Where an ERDS makes use of the processes or technologies outlined in this document, the standards specified shall apply. Irrespective of an ERDS design, the minimum requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met. For example, the approach described in Section 1.2.2, Type 2 ERDS, does not necessarily require a login process or even a dedicated server. However, the processes for protecting the ERDS payloads, i.e. encrypting and signing, shall conform to Section 4.2, Minimum Security Requirements. An ERDS that employs a login process shall also conform to Section 4.3.1, Access Control. An ERDS employing one or more servers shall also conform to Section 4.3, Additional Security Requirements for Type 1 ERDS.

1.3.5 ERDS Operating Procedures

The County Recorder shall have ERDS operating procedures prepared, maintained, and followed that explain the proper operation, management, administration, content restrictions,

and use of their ERDS. ERDS operating procedures shall provide additional details where required by the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Additionally, ERDS operating procedures shall identify, define, or otherwise explain ERDS-design dependent details that are not specifically addressed in this document. ERDS operating procedures shall be sufficient for a Computer Security Auditor to conduct computer security audits.

2 DATA ARCHITECTURE

This section defines the payload contents and structure to be delivered, and when applicable, returned via an ERDS. An ERDS not only includes mechanisms for transporting Type 1 and/or Type 2 instruments, but also provides for the transport of uniform index information, as well as, information about the electronic signature of a notary. An ERDS also provides for the return, when applicable, of Type 1 and/or Type 2 instruments. Irrespective of the ERDS design, the minimum security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met by protecting the ERDS payload structure and content.

2.1 THE ERDS PAYLOAD

All ERDS shall employ a modular payload structure, termed the "ERDS payload", as shown in Figure 2 - ERDS Payload Structure. Modular construction shall allow any content within Type 1 and/or Type 2 instruments. A County Recorder shall list any restrictions on content in each contract with an Authorized Submitter.

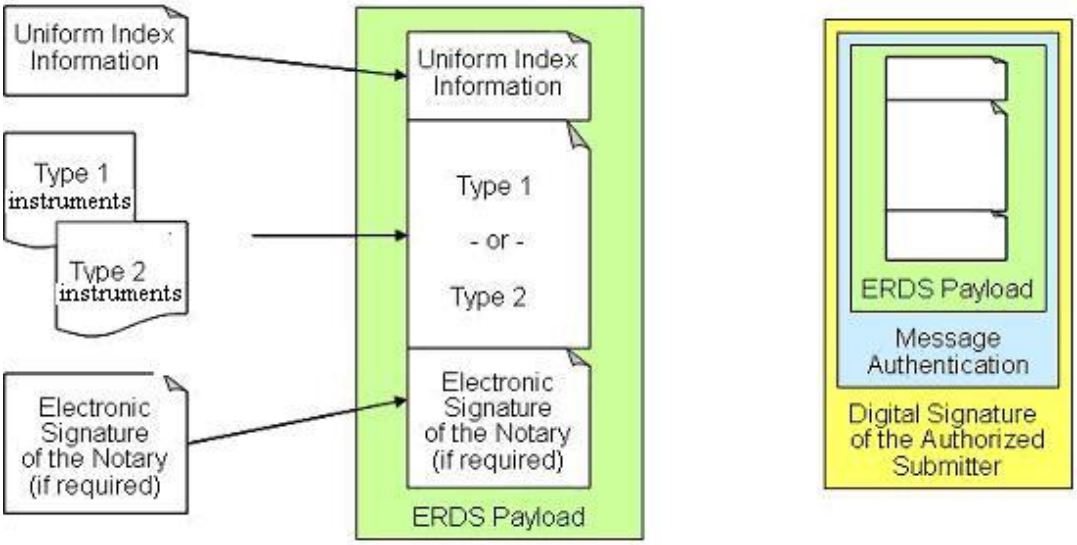

Figure 2 - ERDS Payload Structure

2.2 ERDS PAYLOAD STRUCTURE

The standard structure of an ERDS payload shall consist of three components. The ERDS payloads may contain more components, but, at a minimum, standard ERDS payloads shall contain a component for each of the following:

1. Uniform index information.
2. One or more Type 1 or Type 2 instruments.
3. Information about the electronic signature of a notary.

Each ERDS payload shall be used to generate the Digital Signature of the individual preparing the ERDS payload. When the ERDS payloads are being prepared for delivery to a County Recorder, the Digital Signature shall be of the Authorized Submitter. When the ERDS payloads are being returned to an Authorized Submitter, the Digital Signature shall be of the County Recorder Designee. (Refer to Table 6 - Role Descriptions) This digital signature should not be

confused with the electronic signature of a notary or information about the electronic signature of a notary, but shall be transmitted and stored with the ERDS payload to which it pertains.

The ERDS payloads shall be constructed using a technology suitable for encrypting (as described in Sections 3, ERDS Processes and 4, Security Requirements), transmitting and storing the entire ERDS payload with the digital signature of the Authorized Submitter or the County Recorder Designee preparing the ERDS payload.

Regardless of the ERDS design:

1. All ERDS payloads shall contain the standard components defined in this section.
2. The entire ERDS payload shall be used to generate the digital signature of the Authorized Submitter or the County Recorder Designee.
3. The digital signature of the Authorized Submitter or the County Recorder Designee shall be transmitted and stored with the ERDS payload to which it pertains.

Note: While the ERDS payload structure shall include uniform index information and information about the electronic signature of a notary, their use is detailed in Sections 2.4, Uniform Index Information and 2.5, Electronic Signature of A Notary, respectively.

2.3 TYPE 1 AND/OR TYPE 2 INSTRUMENTS

These specifications do not limit the content or format of Type 1 and/or Type 2 instruments. An ERDS may be used to deliver any industry-standard or non-standard file format acceptable to the County Recorder; including, but not limited to: TIFF, GIF, JPEG, WMV, DOC, PDF, TXT, HTML, XML, or any other file format. Content restrictions shall be defined in the County Recorder's ERDS operating procedures and/or provided for in the ERDS design. Issues such as file format or size, color (versus black and white), graphics resolution, and other characteristics of Type 1 and Type 2 instruments are ERDS-design dependent and shall be at the discretion of the County Recorder.

The ERDA refers to two types of instruments that may be delivered as Type 1 and/or Type 2 instruments. For the purposes of ERDS, these instruments are categorized as "Type 1" and "Type 2". A "Type 1" instrument is defined to mean an instrument affecting a right, title, or interest in real property. A "Type 2" instrument is defined to mean an instrument of reconveyance, substitution of trustee, or assignment of deed of trust. The real estate industry refers to Type 1 and/or Type 2 instruments as "front-end" and "back-end" documents, respectively. Because these terms do not necessarily reflect the method of delivery (digital or digitized), the payload structure, or the file format of the document, the County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type to meet the requirements of the ERDA. A summary of the relationships among statutory, industry, and technology terms is provided in Table 1 - Instrument Types.

Table 1 - Instrument Types

INSTRUMENT TYPE	TYPE 1	TYPE 2
Statute	ERDA Government Code Section 27395	ERDA Government Code Section 27397.5(a)
Purpose	Affect a right, title, or interest in real property	Instrument of reconveyance, substitution of trustee, or assignment of deed of trust

Industry Term	Front-end	Back-end
Method	Digitized	Digital or Digitized
File Format	ERDS-design dependent	ERDS-design dependent
Criminal Record Background Check	Requires fingerprinting	Does not require fingerprinting
Payload Structure	Encrypted and hashed	Encrypted and hashed

The content of Type 1 and Type 2 instruments shall be as follows:

1. Type 1 Instruments; those affecting a right, title, or interest in real property, shall be delivered as digitized electronic records.
2. Type 2 Instruments; instruments of reconveyance, substitution of trustee, or assignment of deed of trust, shall be delivered as digitized electronic records or digital electronic records.

2.4 UNIFORM INDEX INFORMATION

All Type 1 or Type 2 instruments delivered via an ERDS, shall be capable of including uniform index information in the ERDS payload. The County Recorder shall decide on the contents of the uniform index information.

2.5 ELECTRONIC SIGNATURE OF A NOTARY

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

1. The name of the notary.
2. The words ‘‘Notary Public”.
3. The name of the county or other administrative district of a state where the bond and oath of office of the notary are filed.
4. The sequential identification number assigned to the notary, if given.
5. The sequential identification number assigned to the manufacturer or vendor of the notary’s physical and/or electronic seal, if available.

3 ERDS PROCESSES

This section describes the processes for handling the ERDS payloads (i.e. login and transactions). Processes that are employed shall conform to the requirements described in this section. ERDS that include one or more servers shall conform to all of the process requirements in this section. Authorized Access ERDS that do not include a server shall, at a minimum, conform to Sections 3.2, ERDS Payload Submission Process and 3.3, ERDS Payload Retrieval Process. ERDS that include automated processing shall also conform to Section 3.4, Processing Multiple Transactions. Regardless of how an ERDS is implemented, the security and testing requirements outlined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

For each of the diagrams in this section, a gray hexagonal shape represents an interaction between a user and an ERDS. A white rounded rectangle indicates a process performed within an ERDS. The numbers correspond to the descriptions given in the tables following each diagram.

3.1 ERDS LOGIN PROCESS

An ERDS login process is depicted in Figure 3 - Login Process and described in Table 2 - Login Process Description. The login process is substantially the same for both the Authorized Submitter and the County Recorder Designee, to include the use of digital signatures for the purpose of authenticating users. (Refer to Sections 4.2.4, Certificate Authority and PKI and 4.3.1.2, Authentication Requirements for more information about ERDS authentication requirements.)

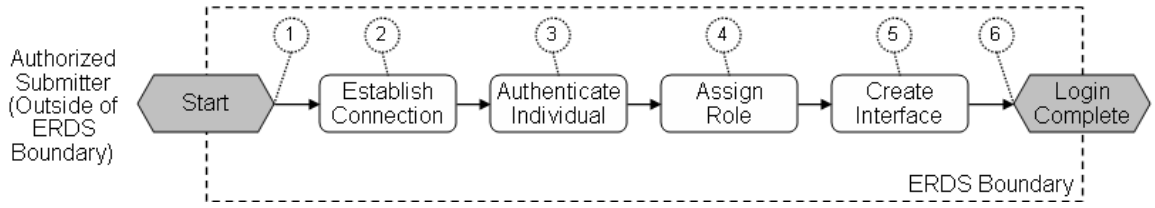

Figure 3 - Login Process

While the login process described in this document refers to the actions of, and subsequent responses to, a single user, the design of an ERDS may support multiple, simultaneous connections to and from multiple users. Each individual user shall be limited to one, and only one, active login session under a single ERDS user account. An individual user may have multiple screens active and displayed simultaneously, but all screens active for a user account shall be attributable to an active login session associated with that user account.

Table 2 - Login Process Description

	PROCESS	DESCRIPTION
1	Start	A user navigates to an ERDS. The identity of the user has not yet been established.
2	Establish Connection	ERDS establishes a secure connection with the user. Even though the identity of the user has not yet been established, this connection is intended to protect the user's password.
3	Authenticate Individual	Once a secure Internet session is established, the user is prompted for a user ID and password. ERDS provides a login screen and authenticates credentials entered by the user. If authentication fails, ERDS returns to the login screen and indicates that access is not authorized. If the user ID and password are authenticated, the user is prompted to confirm their identity using a digital signature. A proxy connection is established between the user and the ERDS server. Credentials and control of the session are transferred to the ERDS server. The ERDS server shall control authentication of the digital signature.
4	Assign Role	If the digital signature is authenticated, the identity of the user has been established. ERDS determines what role the user is authorized. Having determined a role, ERDS assigns privileges associated with that role for the duration of the session.
5	Create Interface	ERDS application software starts. ERDS builds an interface for the session based on the assigned role of the user.
6	Login Complete	The interface created for the session is presented to the user. The login process has completed. The ERDS server starts a timer for the session. If another command is not received before the timer reaches a timeout limit, the session shall be terminated.
	Logout	Secure sessions shall be terminated if the authenticated user logs out or after a preset timeout limit, whichever occurs first. (For preset timeout limit criteria, refer to Section 4.5.2, Incident Response Procedures.)

3.2 ERDS PAYLOAD SUBMISSION PROCESS

An ERDS payload submission process is depicted in Figure 4 - Payload Submission Process and described in Table 3 -Payload Submission Process Description. The process of an Authorized Submitter submitting an ERDS payload is substantially the same as a County Recorder Designee returning an ERDS payload. For the purposes of this section, a user is described as either a Sender or Recipient. A Sender is a user who is submitting an ERDS payload via the ERDS. A Recipient is a user who is retrieving ERDS payloads from the ERDS.

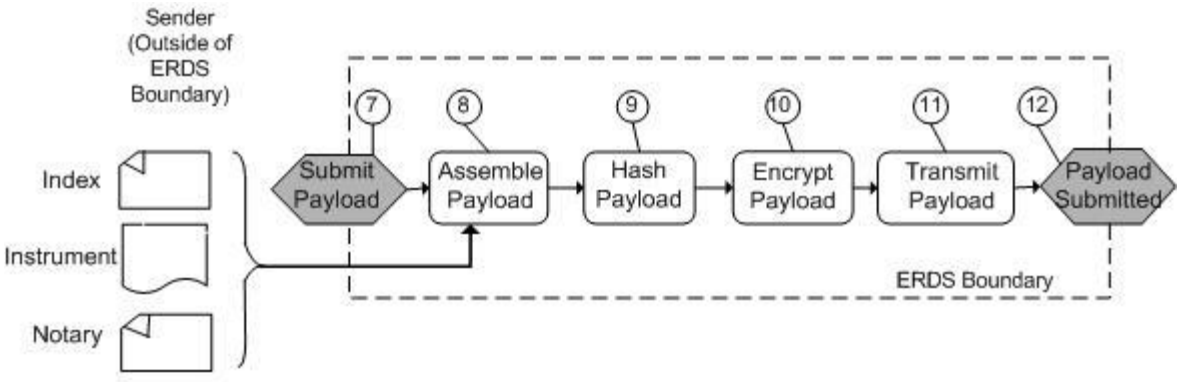

Figure 4 - Payload Submission Process

Table 3 - Payload Submission Process Description

	PROCESS	DESCRIPTION
7	Submit Payload	The Sender indicates that a Type 1 or Type 2 instrument is ready to be submitted. Prior to this event, the Sender enters, selects or otherwise indicates the contents to be placed in an ERDS payload. For the return process, this step indicates that a Type 1 or Type 2 instrument is ready to be returned.
8	Assemble Payload	The ERDS interface collects the content into an ERDS payload structure.
9	Hash Payload	The ERDS payload is hashed to generate a message digest. This digest shall be used to (1) generate the digital signature of the Sender and (2) detect unauthorized changes that occur either during transmission to, or while in storage on, the ERDS server. The digital signature shall be submitted together with the ERDS payload. Note: The digital signature of the Sender is created by using the private key of the Sender to encrypt the message digest. Using the private key of the Sender assures the Recipient that the message digest was generated by the Sender.
10	Encrypt Payload	The ERDS interface encrypts the ERDS payload together with the digital signature of the Sender.
11	Transmit Payload	The ERDS interface relays the encrypted ERDS payload to the ERDS server.
12	Payload Submitted	For the Sender, the ERDS server acknowledges receipt of the encrypted ERDS payload and the ERDS interface indicates that transmission to, and storage on, the ERDS Server was successfully completed. If either transmission or storage failed, the ERDS interface indicates that transmission or storage failed. (Specific reasons for failure, transmission timeout and storage limits, and the text of error messages are ERDS-design dependent.) For a Recipient, this event indicates an ERDS payload has been submitted by a Sender and is ready for inspection.

3.3 ERDS PAYLOAD RETRIEVAL PROCESS

An ERDS payload retrieval process is depicted in Figure 5 - Payload Retrieval Process and described in Table 4 - Payload Retrieval Process Description. The process of retrieving a payload is substantially the same for both the Authorized Submitter and County Recorder Designee. For the purposes of this section, a user is described as either a Sender or Recipient. A Sender is a user who is submitting an ERDS payload to the ERDS. A Recipient is a user who is retrieving the ERDS payloads from the ERDS.

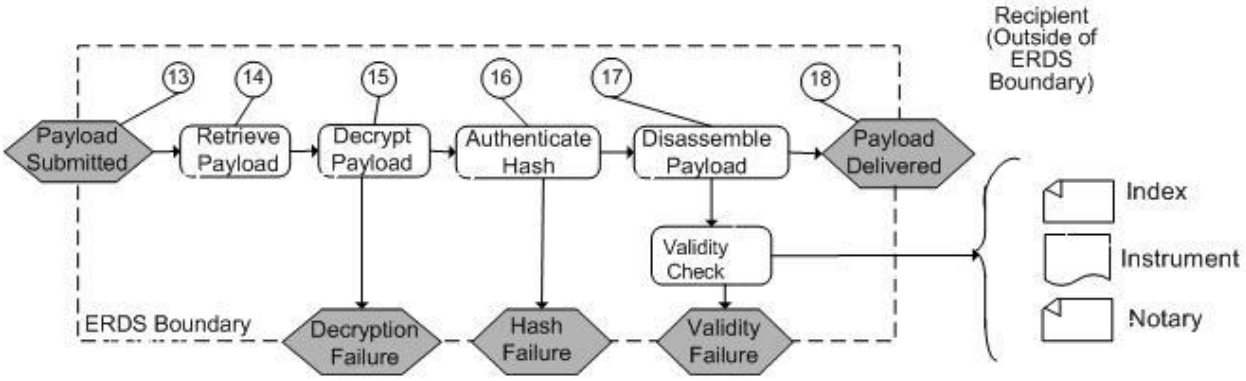

Figure 5 - Payload Retrieval Process

Table 4 - Payload Retrieval Process Description

	PROCESS	DESCRIPTION
13	Payload Submitted	For the Sender, the ERDS server acknowledges receipt of the encrypted ERDS payload and the ERDS interface indicates that transmission to, and storage on, the ERDS server was successfully completed. If either transmission or storage failed, the ERDS interface indicates that transmission or storage failed. (Specific reasons for failure, transmission timeout and storage limits, and the text of error messages are ERDS-design dependent.) For a Recipient, this event indicates an ERDS payload has been submitted by a Sender and is ready for inspection.
14	Retrieve Payload	If authorized, the Recipient indicates that an ERDS payload should be retrieved. The ERDS interface downloads the ERDS payload to a location indicated by the Recipient.
15	Decrypt Payload	The ERDS interface decrypts the ERDS payload together with the digital signature of the Sender. If the decryption fails, the ERDS interface indicates that the decryption failed. (Specific reasons for failure and the text of error messages are ERDS-design dependent.)
16	Authenticate Hash	The ERDS interface uses the public key of the Sender to decrypt the digital signature of the Sender and recover the digest of the ERDS payload. The ERDS interface hashes the ERDS payload and generates a second digest to compare with the digest recovered from the digital signature of the Sender. If the two digests are not identical, the ERDS interface indicates that a hash failure occurred. If an active session is still connected to the ERDS server, the ERDS interface transmits a message back to the ERDS server indicating a hash failure occurred.

	PROCESS	DESCRIPTION
17	Disassemble Payload	If the two digests are identical, the ERDS interface extracts the contents of the ERDS payload and performs a validity check to ensure the contents are free of malware. The anti-malware interface warns the Recipient if the contents are not free of malware. (Specific anti-malware interfaces, the text of error messages, and actions allowed in response to a malware warning are ERDS-design dependent.) If the contents are free of malware, the ERDS interface prompts the Recipient for a location to store the contents.
18	Payload Delivered	The ERDS interface indicates that the ERDS payload was successfully delivered.

3.4 PROCESSING MULTIPLE TRANSACTIONS

In implementing an ERDS, the County Recorder may add capabilities to process multiple Type 1 or Type 2 instruments. As examples, and for illustrative purposes only, an ERDS may be designed to process multiple Type 1 or Type 2 instruments in any or all, of the following ways:

1. By inserting multiple Type 1 or Type 2 instruments into a single ERDS payload.
2. By repeated processing of Type 1 or Type 2 instruments from a single source, such as a scanner or directory.
3. By repeated processing of Type 1 or Type 2 instruments based on a list of file locations.

The automated processing of multiple Type 1 or Type 2 instruments is subject to the following restrictions:

1. Repeated processing from a single source or a list of files shall result in separate ERDS payloads – one for each file.

Additionally, a County Recorder may establish an automated process that retrieves, decrypts, and checks the contents of submitted ERDS payloads. The details of implementing such an automated process are ERDS-design dependent; however, the security and testing requirements outlined in this document shall be met.

4 SECURITY REQUIREMENTS

This section describes the security requirements for protecting an ERDS. Processes and technologies employed in implementing an ERDS, pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, shall conform to the requirements as defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. All ERDS shall conform to Section 4.2, Minimum Security Requirements. Regardless of how an ERDS is implemented, the security and testing requirements outlined in this document shall be met.

This section details the baseline requirements and standards for administrative, physical and technical security controls.

4.1 INTRODUCTION

The security of any system is implemented through a combination of administrative, physical, and technical controls. Administrative controls protect the security of systems by implementing management policies and procedures. Physical controls protect the security of systems by limiting physical access to hardware and media. Technical controls protect the security of systems by limiting logical access to software and data. For an ERDS, technical controls protect the integrity of system configurations and the security of information contained in Type 1 and Type 2 instruments.

4.1.1 Conceptual Overview

ERDS shall protect the security of data, both in transmission and storage, on ERDS-designated components, as well as, provide mechanisms to detect unauthorized changes and verify the integrity of information contained in the ERDS payloads.

For illustrative purposes, a diagram showing the major components of an ERDS are depicted in Figure 6 - Conceptual Security Infrastructure and described in Table 5 - Conceptual Security Infrastructure Descriptions. Actual ERDS implementations may vary from the configuration depicted in Figure 6 - Conceptual Security Infrastructure. Implementation details are at the discretion of the County Recorder; however, all requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be required for system certification.

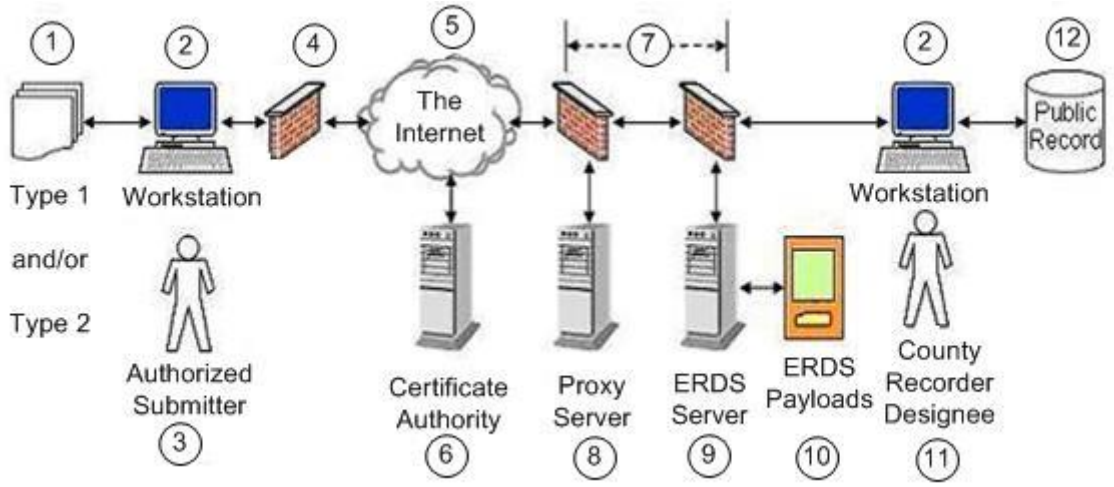

Figure 6 - Conceptual Security Infrastructure

Table 5 - Conceptual Security Infrastructure Descriptions

	COMPONENT	DESCRIPTION
1	Type 1 and/or Type 2 instruments	Type 1 and/or Type 2 instruments prepared for submission. The preparation of Type 1 and/or Type 2 instruments is not a process within an ERDS.
2	Workstation	A computer used to connect to, and interact with, an ERDS
3	Authorized Submitter	A party and his/her employees that has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.
4	Authorized Submitter Network	The network an Authorized Submitter uses to connect to an ERDS. Networks shall meet the minimum security requirements described in Section 4.3.3, Network Security.
5	The Internet	A global network of computer systems interconnected through the use of commonly accepted protocols standardized through the Internet Engineering Task Force.
6	Certificate Authority	A certificate authority issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.
7	County Recorder Network	The network a County Recorder Designee uses to connect to an ERDS. Networks shall meet the minimum security requirements described in Section 4.3.3, Network Security.
8	Proxy Server	Server that functions as the interface between an Authorized Submitter and an ERDS server.
9	ERDS Server	Computer hardware, software, and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the ERDS application software. It includes software for encrypting, decrypting, hashing, submitting, and when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that ERDS server functions can be isolated from other server functions, as evidenced by audit
10	ERDS Payloads	An electronic structure designed for the purpose of delivering digital electronic records or digitized electronic records to a County Recorder via an ERDS. The structure is also used to return, when applicable, digital electronic records or digitized electronic records to an Authorized Submitter via an ERDS.

	COMPONENT	DESCRIPTION
11	County Recorder Designee	A Secure Access role assigned by the County Recorder to retrieve and when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting
12	Public Record	The repository of Type 1 and Type 2 instruments. An ERDS shall have no capabilities to modify, manipulate, insert, or delete information in the public record. The public record is outside of the ERDS boundary and is depicted for illustrative purposes only.

4.2 MINIMUM SECURITY REQUIREMENTS

All ERDS, for Type 1 and Type 2 instruments, shall employ the minimum security requirements described in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Additional security requirements for Type 1 ERDS are contained in Section 4.3, Additional Security Requirements for Type 1 ERDS.

All ERDS:

1. Shall employ up-to-date anti-malware software.
2. Shall employ cryptography, including hashing, encryption, and decryption.
3. May not employ either compromised or weak encryption algorithms.
4. May not contain known vulnerabilities.
5. May not be susceptible to published exploits.

Standards and guidelines established in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 included in this document are based on Federal Information Processing Standards (FIPS) and National Institute of Standard and Technology (NIST) publications including: NIST Special Publication 800-88, Guidelines for Media Sanitization (publication date September 2006); FIPS 180-4, Secure Hash Standard (publication date March); FIPS 140-2, Security Requirements for Cryptographic Modules (publication data 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 July 2008); NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date August 2013); NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date February 2011); FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013).

4.2.1 Data Integrity

All ERDS for either Type 1 or Type 2 instruments shall assure submitted documents do not contain content that draws data or images from sources external to the digital electronic record and/or digitized electronic record. Prior to submitting, or when applicable, returning an ERDS payload, content shall be scanned and or reviewed for active content including; but, not limited to, the following:

1. Viruses
2. Worms
3. Trojan Horses

4. Spyware
5. Adware
6. ActiveX components
7. Java Script
8. Java components
9. HTML encoded hyperlinks
10. Any other executable software

All ERDS shall employ up-to-date anti-malware software on all workstations and servers employed for processing ERDS payloads. Active content detected by anti-malware shall be removed as soon as it is detected. Active content that cannot be removed shall be disabled. The technologies employed and the points in the delivery process where active content is removed and/or disabled are ERDS-design dependent.

4.2.2 Payload Protection

4.2.2.1 Payload Confidentiality

4.2.2.2 All ERDS for 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. The encryption algorithms approved for ERDS are specified in CCR Title 11, Division 1, Chapter 18, § 999.137 (a). Payload Integrity

All ERDS for Type 1 or Type 2 instruments, shall use hashing to protect the integrity of the ERDS payloads. The hash function approved for the ERDS payloads is the Secure Hash Algorithm (SHA) defined in CCR Title 11, Division 1, Chapter 18, § 999.137 (b).

4.2.2.3 Payload Authenticity

All ERDS for Type 1 or Type 2 instruments, shall use Digital Signatures to assure the authenticity of ERDS payloads. Hash values that are encrypted using asynchronous techniques are known as Digital Signatures. The signing functions approved for ERDS payloads are defined in the CCR Title 11, Division 1, Chapter 18, § 999.137 (c).

4.2.3 Cryptographic Key Generation

Cryptographic modules used for generating encryption keys shall meet the requirements of Security Level 2 defined in FIPS 140-2, “Security Requirements for Cryptographic Modules” (publication date May 2001, with a change notice dated December 2002).

4.2.4 Certificate Authority and PKI

The County Recorder shall establish a Public Key Infrastructure (PKI) to ensure all ERDS users are uniquely identified and to protect the integrity and authenticity of ERDS payloads. The County Recorder shall determine and implement a PKI strategy based on the following guidelines:

1. The RSA Algorithm using a minimum key-length of 1024 bits.
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).

A public/private key-pair shall be generated for each user authorized a role in handling ERDS payloads. In a PKI, public and private keys are used in encryption, decryption and signing processes. Cryptographically-related keys are referred to as a public/private key pair.

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

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

For Type 1 instruments, authentication shall consist of two factors: (1) the user ID and password associated with an approved user account and (2) the user's PKI identity credentials. For Type 2 instruments, authentication shall be based on the user's PKI identity credentials.

Resources and means for establishing a PKI for either Type 1 or Type 2 instruments shall be at the discretion of the County Recorder; but, commercially available certificate authorities, if employed, may be on the list of certification authorities approved by the California Secretary of State. The California Secretary of State maintains an approved list of digital signature certification authorities at http://www.sos.ca.gov/digsig/digsig.htm.

4.2.5 Securing ERDS Payloads

The process of securing ERDS payloads for Type 1 or Type 2 instruments during submission is shown in Figure 7 - Securing ERDS Payloads. The process of securing the ERDS payloads during and when applicable, the return, is identical except for the use of encryption keys. The configuration and algorithms depicted in Figure 7 are for illustration purposes only; however, all ERDS shall encrypt the ERDS payloads.

After an Authorized Submitter has created an ERDS payload, the ERDS payload is hashed using SHA. The resulting hash value, called a digest, is encrypted using RSA and the private key of the Authorized Submitter ─ creating the digital signature of the Authorized Submitter.

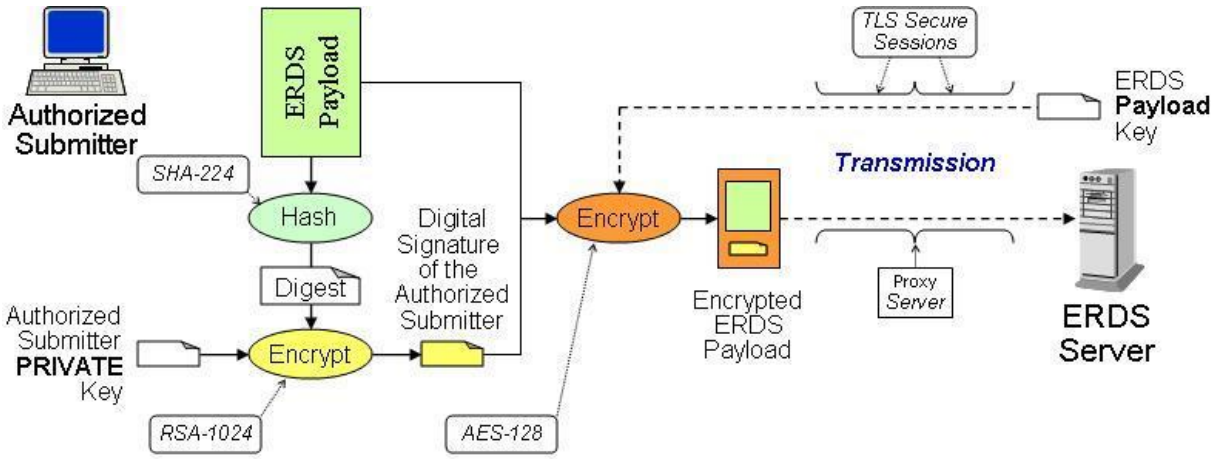

Figure 7 - Securing ERDS Payloads

The ERDS payload and digital signature of the Authorized Submitter are encrypted using AES and the ERDS Payload Key, delivered from an ERDS server. The ERDS Payload Key is stored on an ERDS server so that a County Recorder Designee can decrypt the ERDS payload.

(Note: In an ERDS, the Payload Key is the public key of a County Recorder public/private key-pair.)

The encrypted ERDS payload is transmitted to and stored on an ERDS server. Encrypted ERDS payloads are relayed through the proxy server which acts as a proxy between the Authorized Submitter and the ERDS server. The ERDS server receives and stores encrypted ERDS payloads, so that a County Recorder Designee can use the ERDS Payload Key to decrypt the ERDS payload. (Note: In an ERDS, the County Recorder Designee shall need to use the private key of a County Recorder public/private key-pair.)

4.2.6 Validating ERDS Payloads

The process of validating the ERDS payloads for Type 1 or Type 2 instruments is shown in Figure 8 - Validating ERDS Payloads. The process of validating the ERDS payloads during return, when applicable, is identical except for the use of encryption keys. The configuration and algorithms depicted in Figure 8 are for illustration purposes only.

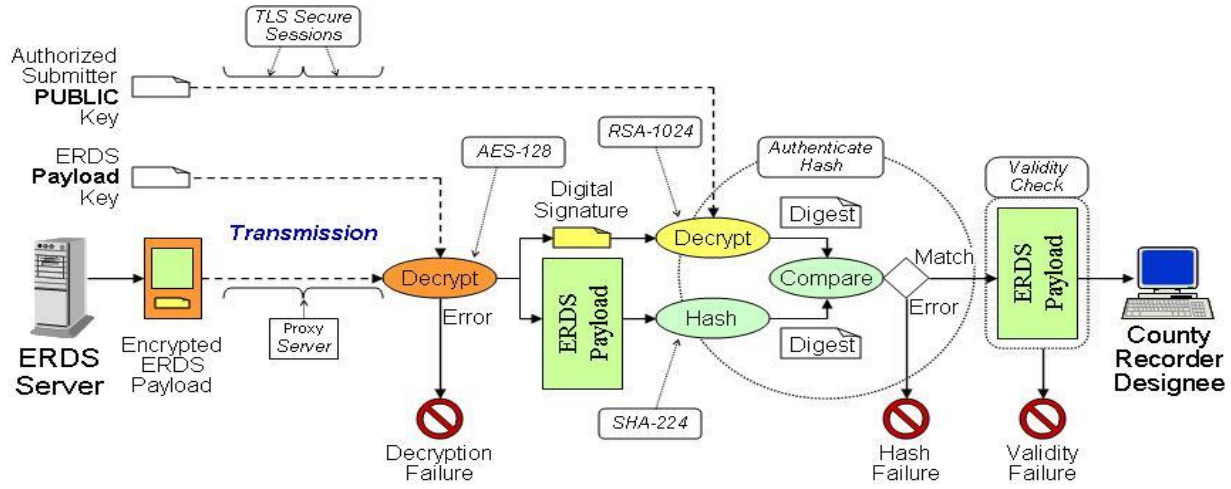

Figure 8 - Validating ERDS Payloads

The decryption, hash authentication and validity checking of the ERDS payloads are ERDS-design dependent. Decryption and hash authentication processes complement the corresponding encryption and signing processes, respectively. Validity checking is based on the contents of the ERDS payload. However, all ERDS shall generate and log errors for decryption, hash authentication and validity check failures.

4.2.7 Workstation Security

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

1. Anti-malware software configured to start on system boot-up.
2. Operating system software with the most up-to-date patches and hot-fixes.
3. Host-base firewall configured to restrict inbound and outbound connections.

For ERDS that serve Type 1 instruments only, installed applications shall be limited to the purpose of performing the necessary operational needs of the recording process as defined by the County Recorder. The County Recorder shall include this requirement as a mandatory

provision in all contracts with Authorized Submitters whom shall ensure that an Agent, if any, complies with these requirements. The contents of the contract provision are subject to audits and local inspections.

4.2.8 Media Security

The ERDS payloads and encryption keys for either Type 1 or Type 2 instruments shall be encrypted when stored on any storage media. The encryption employed for protecting the ERDS payloads and encryption keys in storage, shall conform to the standards for transmitting the ERDS payloads as described in Section 4.2.2, Payload Protection.

Storage media includes, but is not limited to, fixed disks, removable disks and portable devices. Fixed and removable disks for either Type 1 or Type 2 instruments, shall be sanitized as defined in NIST Special Publication 800-88, "Guidelines for Media Sanitization" publication date September 2006), prior to reallocating ERDS hardware or storage media to other purposes.

Unauthorized access or changes to storage media and improper sanitization of storage media shall be reported as required in Section 4.5.2, Incident Response Procedures.

4.3 ADDITIONAL SECURITY REQUIREMENTS FOR TYPE 1 ERDS

This section describes additional security requirements that shall be implemented for Type 1 ERDS. ERDS that include one or more servers shall conform to all of the security requirements in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

This section describes the security requirements that shall be implemented for Type 1 ERDS that delivers Type 1 instruments. Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, Type 1 instruments shall meet the security requirements in Section 4.2, Minimum Security Requirements, and additionally meet the requirements specific to Type 1 instruments described in this Section. ERDS that serve both Type 1 and Type 2 instruments shall be required to meet the additional security requirements of Type 1 instruments.

4.3.1 Access Control

A combination of security mechanisms shall be applied to protect the safety and security of the ERDS. Access control failures shall be logged and/or documented and reported according to Section 4.5.2, Incident Response Procedures.

4.3.1.1 Identification Requirements

Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, ERDS that serve Type 1 and Type 2 instruments shall be required to meet the following additional identification security requirements required for Type 1 instruments. For ERDS that serve Type 1 instruments, authentication shall consist of two factors: (1) the user ID and password associated with an approved user account and (2) the user's PKI identity credentials (as defined in Section 4.2.4, Certificate Authority and PKI).

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

1. Each ERDS user shall be uniquely identified.
2. Shared user accounts and identity credentials shall be prohibited.
3. User IDs shall either be based on the verified name of the user or a pseudonym approved by the County Recorder.

4. User accounts shall be associated with ERDS roles.

4.3.1.2 Authentication Requirements

Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, ERDS that serve Type 1 and Type 2 instruments shall be required to meet all of the additional authentication security requirements required for Type 1 instruments. The standard for electronic authentication shall be based on NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013). NIST defines electronic authentication as "the process of establishing confidence in user identities electronically presented to an information system."

Authentication shall meet the following requirements:

1. The standard for electronic authentication shall employ two factors: (a) a token containing a cryptographic key (e.g. a digital certificate) issued to the user and (b) a password associated with the user ID.
2. Authentication assurance shall meet Level 3 or higher, as defined in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013).
3. Any of the token methods described in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013), may be used provided that authentication assurance Level 3 or higher is achieved.

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

4.3.1.3 Authorization Requirements

Access to the ERDS payloads shall be based on the authorization standards defined in this section. The ERDS payloads submitted by an Authorized Submitter or Agent shall be retrievable by any County Recorder Designee.

4.3.1.3.1 Role-Based Access Control

Access to an ERDS that serve either Type 1 or Type 2 instruments shall be controlled using a role-based access control system. Textual disclaimers or verbal disclaimers alone shall not be sufficient to control access to digital electronic records and digitized electronic records under the control of an ERDS. A role is defined as a security mechanism, method, process or procedure that defines specific privileges controlling the level of access to an ERDS. ERDS roles are described in Table 6 - Role Descriptions.

Table 6 - Role Descriptions

Role	Description
Authorized Access	A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.
Computer Security Auditor	(1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vender of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.
County Recorder Designee	A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return of the submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
ERDS Account Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure accounts, assign roles, and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
ERDS System Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings, and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.
Physical Access	Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.
Secure Access	A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator who is authorized to configure hardware, software, and network settings; 4) an ERDS Account Administrator who is authorized to configure accounts, assign roles, and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return the submitted ERDS payloads.

Role	Description
Vendor of ERDS Software (or Developer)	A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resource used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.

Irrespective of design, the access control system shall control the following characteristics:

1. Whether or not a session may be established with an ERDS.
2. What ERDS payloads will be displayed.
3. Whether or not the ERDS payloads may be submitted, retrieved, and, when applicable, returned.
4. Whether Type 1 or Type 2 instruments may be included within an ERDS payload.

The County Recorder may define limits, if any, on the day of the week and time of day ERDS transactions can be conducted. Limits may be implemented as part of the access control system or be set by contract or agreement.

The County Recorder shall also be responsible for controlling the assignment of user accounts and identity credentials. User accounts and identity credentials shall be issued to the person, and a role shall be assigned to control transactions performed under that user account. The security system shall be capable of controlling this electronic access based on the roles authorized at the time a user successfully logs into an ERDS. Persons granted access shall be subject to fingerprinting depending on the role requested.

Shared user accounts may not be issued. At no time shall more than one person be authorized access to an ERDS using a single ERDS user account or set of identity credentials. Each person shall be uniquely identified. If a user's status changes, so that access to an ERDS is no longer required, the user's ERDS account and identity credentials shall be disabled and revoked for the purposes of an ERDS. ERDS user accounts and identity credentials are non-transferable.

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

ERDS users may be authorized multiple roles. The security system shall be capable of controlling access based on the roles authorized at the time a user successfully logs into an ERDS. Whereas one ERDS may be used in a collaborative system, the security system of a Multi-County ERDS shall be capable of controlling access based on the county to which the ERDS payloads are to be delivered and, when applicable, returned. (Refer to Section 1.3.2, Functionality, for more information about Multi-County ERDS.)

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

not be granted access to the ERDS payloads unless authorized by the County Recorder. (Refer to Section 4.3.4, Physical Security.)

4.3.1.3.2 Authorized Submitter and Agent

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

An Agent named in more than one contract with a County Recorder shall be required to indicate which Authorized Submitter is represented in a transaction. An ERDS shall control Agent transactions through the use of unique credentials (user ID, password, and token) or other means, provided that an accounting of transactions can be provided to the Authorized Submitter on whose behalf the Agent is acting.

Authorized Submitters may employ a third-party vendor as an Agent provided that the third-party vendor is neither a Computer Security Auditor nor a Vendor of ERDS Software. (Refer to the definition of "Agent" in Section 7, Acronyms and Definitions)

4.3.1.4 Accountability Requirements

Auditable ERDS events shall be logged for purposes of audit, local inspection and review, incident response and reporting. Auditable events may be logged using automated or manual processes. Logs shall be safely stored and maintained in a manner that ensures their availability for a period of at least 24 months, or at least one computer security audit, whichever occurs later. Incident response and reporting requirements are detailed in Section 4.5.2, Incident Response Procedures.

4.3.1.4.1 Session Activities

For Type 1 instruments, the following authorized activities shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Login successes and failures.
2. Sessions starts and ends.
3. Session timeout (e.g. inactive in excess of 30 minutes).
4. The ERDS payload transactions submittals, retrievals, and when applicable, returns (as described in Section 4.3.1.4.3, Transaction Activities).

4.3.1.4.2 Unauthorized Activities

For Type 1 instruments, the following unauthorized activities shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

Unauthorized access attempts, including, but not limited to:

1. Unauthorized users attempting access, either physical or logical to ERDS storage areas.
2. Any user attempting to use ERDS software and/or interfaces in a non-ERDS manner.

For Type 1 and Type 2 instruments, the use of expired or revoked credentials shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

4.3.1.4.3 Transaction Activities

For Type 1 and Type 2 instruments submitted, retrieved and when applicable, returned, the following transaction activity information shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Unique name of the ERDS payload.
2. Dates and times the ERDS payload was submitted, retrieved, and when applicable, returned.
3. Identity of the individual who submitted, retrieved and when applicable, returned the ERDS payload.
4. Name of the organization that the individual represented while submitting, retrieving and when applicable, returning the ERDS payload.
5. Success or failure of decryption, hash failure, and validation.

Note: The unique name of the ERDS payload is ERDS-design dependent.

4.3.1.4.4 Accountability Failures

Auditable events shall never overwrite other logged events. Additionally, ERDS servers shall not accept Type 1 or Type 2 instruments if:

1. Auditable events cannot be logged.
2. Logs consume 95% or more of the storage space allocated for logging.
3. Logs cannot be safely stored.

4.3.1.5 Administration Requirements

A County Recorder shall establish ERDS operating procedures for, and have responsibility over, the day-to-day administration of ERDS accounts, roles and cryptographic keys. ERDS administration shall be performed by one or more individuals assigned as the ERDS System Administrator and/or ERDS Account Administrator.

The following administration activities for Type 1 instruments shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not.
2. Hardware and software configuration changes.

Hardware and software configuration changes shall be based on the inventory of all hardware and software installed on, or attached to, an ERDS since the most recent audit.

4.3.2 Server Security

Servers employed for the purpose of implementing an ERDS may be dedicated to ERDS functions or integrated with other servers. Separate physical servers dedicated to performing ERDS server functions are not required, provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.

4.3.2.1 Proxy Server

An ERDS shall employ an ERDS proxy server. The purpose of the proxy server shall be to provide a public interface to an ERDS and provide proxy services between the Authorized Submitter and the ERDS server.

The proxy server shall:

1. Establish secure Internet sessions.
2. Authenticate user ID and password credentials.
3. Transfer and/or relay ERDS requests received via authenticated secure Internet sessions to the ERDS Server.
4. Be physically and logically separated from the ERDS server.

Proxy servers may not execute an ERDS functionality except as described above.

4.3.2.2 ERDS Server Security

The ERDS server shall communicate via secure sessions through the proxy server when interoperating via the Internet. At a minimum, sessions between the proxy server and the ERDS server shall be protected using a secure protocol, as defined in Section 4.3.3.1, Transmission Security/Confidentiality. Direct logins from the Internet to an ERDS server is prohibited.

The ERDS server shall:

1. Run the ERDS application software.
2. Store the ERDS payloads.
3. Authenticate the ERDS credentials.
4. Control the ERDS access based on assigned roles.
5. Log the ERDS transactions.

4.3.2.3 Server Hardening

ERDS servers shall be configured to prevent unauthorized access, modification or use. The County Recorder shall establish standards for "hardening" servers by selecting a checklist or guideline and customizing it to meet the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

The County Recorder shall ensure that all county servers used for an ERDS are "hardened" according to one of the following checklists or guidelines:

1. NIST Special Publication 800-70 Revision 2, Security Configuration Checklists Program for IT Products-Guidelines for Checklist User and Developers (publication date, February 2011).
2. Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.

At a minimum, ERDS servers shall:

1. Be "hardened" according to the standards establish by the County Recorder.
2. Have a host-based file integrity checking system configured to alert the ERDS System Administrator of an operating system file change to the ERDS server.
3. Have anti-malware software installed and operating to protect the server.

4.3.2.4 Server Events

The following server events shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. 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.
2. Events for which the ERDS System Administrator is alerted of possible or actual intrusion.
3. Unauthorized changes to the ERDS operational configuration.
4. Hardware or software configuration changes.
5. For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas.
6. Use of expired or revoked credentials.
7. For Type 1 only, privilege elevation.
8. For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session.
9. ERDS accounts locked out and/or disabled due to failed consecutive login attempts.
10. Auditable events overwrite other logged events.
11. For Type 1 only, ERDS account creation, modification, deletion, suspension, termination or revocation whether authorized or not.
12. A decryption failure.
13. A hash failure.
14. A validity check failure.
15. Type 1 or Type 2 instrument submitted unencrypted.
16. Type 1 instrument submitted as a Type 2 instrument or vice versa.
17. Type 1 instrument submitted via an Authorized Access ERDS.
18. Unauthorized transactions submitted via ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2.
19. For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.
20. Inability to obtain and employ cryptography, including hashing, encryption and decryption.
21. For Type 1 only, discovery of newly published vulnerability existing on a certified ERDS.
22. Discovery of susceptibility to newly published exploit.
23. Inability to obtain and employ the most up-to-date patches and hot-fixes.
24. Any other event that compromises the safety or security of an ERDS.

4.3.3 Network Security

The integrity and reliability of an ERDS depends on security measures applied at the network level. An ERDS shall use a combination of networks, including the Internet. ERDS components shall be protected from unauthorized network activity as described in this section.

4.3.3.1 Transmission Security/Confidentiality

ERDS transactions via any network shall be protected using encryption. Data packets transmitted via networks are easily captured and compromised, if unencrypted. Two basic processes that shall be protected during any ERDS session are the login sequence and the transfer of the ERDS payloads.

Prior to beginning a login sequence, a secure connection shall be established in order to protect passwords. The standard for establishing secure connections is the Transport Layer Security (TLS) protocol as described in NIST Special Publication 800-63-2, "Electronic Authentication " (publication date, August 2013). At 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). ERDS may not employ "Basic" or Hypertext Transport Protocol referred to commonly as "HTTP" authentication to transmit passwords.

Once a secure connection is established and the user authenticated, a proxy connection is established between the user and the ERDS server. Credentials and control of the session are transferred to the ERDS server.

Once established, the secure connection shall be maintained as long as ERDS transactions are conducted. Secure connections shall be terminated if the authenticated user logs out or after a preset timeout limit of not more than 30 minutes, whichever occurs first. (For preset timeout limit criteria, refer to Section 4.5.2, Incident Response Procedures.)

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

4.3.3.1.1 Transmission Integrity

An ERDS shall employ message authentication codes (MAC) to assure the authenticity of encrypted ERDS packets. MACs shall conform to the standard defined in FIPS 198-1, "The Keyed-Hash Message Authentication Code (HMAC)" (publication date, July 2008).

4.3.3.2 Unauthorized Network Traffic

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

1. Employ stateful packet inspection.
2. Block unauthorized connections by limiting connection attempts addressed to the ERDS components to those necessary for ERDS operation.
3. Be designed and configured to fail "closed" rather than "open".
4. Detect possible intrusions; and, if a possible intrusion is detected, alert the ERDS System Administrator and take action to prevent the intrusion.

4.3.3.3 Alternative Transmission Methods

An ERDS may employ alternative transmission methods, which shall meet one of the following standards:

1. Virtual Private Networks (VPNs).
2. "Dedicated circuits" as employed in existing government systems.

Irrespective of an ERDS design, the security and testing requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

4.3.3.4 Network Events

For Type 1 instruments, the following network events shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.
2. Events for which the ERDS System Administrator is alerted of possible or actual intrusion
3. Unauthorized changes to the ERDS operational configuration.

4.3.4 Physical Security

The site housing the ERDS server shall be protected from unauthorized physical access. The server shall be locked in such a manner as to prevent unauthorized physical access. Disks and backup tapes containing ERDS software and/or data (including encryption keys) shall be locked in a cabinet or other container when not in use.

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

At a minimum, ERDS operating procedures and/or agreements shall provide for the following:

1. All requests for physical access to an ERDS server are subject to disapproval by the County Recorder. For an ERDS involving a shared, multi-purpose server, the County Recorder may not have overall authority to approve physical access; however, the County Recorder shall retain disapproval authority in an agreement involving shared multi-purpose servers.
2. Persons who are authorized physical access to an ERDS server require fingerprinting.
3. An inventory that accounts for all keys, whether physical or electronic, used for locking and unlocking physical access to an ERDS server, software and/or data shall be completed at least every 90 calendar days.
4. During audits, the Computer Security Auditor shall be allowed to inspect all access requests and inventory reports that occurred within a 2-year period prior to the start of an audit.
5. During local inspections, ERDS Program staff shall be allowed to inspect all access requests and inventory reports that occurred within a 2-year period prior to the start of a local inspection.

4.4 SECURITY CHECKLISTS

The County Recorder shall select checklists for hardening ERDS components through the "NIST Special Publication 800-70 Revision 2 National Checklist Program for IT Products-Guidelines for Checklist Users and Developers" (publication date February 2011). Selected checklists shall be consistent with the ERDS design.

4.5 INCIDENT RESPONSE

For the purposes of this Section, the following definitions apply:

1. "Auditable" means an auditable ERDS event, as referenced in Section 4.3.1.4, Accountability Requirements.
2. "Incident" means an event that may have compromised the safety or security of an ERDS.
3. "Reportable" means an incident that has resulted in the compromise of the safety or security of an ERDS and shall be reported to the ERDS Program

4.5.1 Incident Reporting

Any incident that compromises the safety or security of an ERDS shall be reported by the County Recorder to the County Board of Supervisors, District Attorney(s), Computer Security Auditor and the ERDS Program according to procedures outlined in the ERDS System Certification Handbook. All incidents shall be documented for inclusion as part of a computer security audit.

4.5.2 Incident Response Procedures

The County Recorder shall establish an ERDS operating procedures for handling and responding to incidents. The ERDS operating procedures shall conform to the requirements listed in Table 7 - Incident Response Criteria and Reporting Requirements. Reportable incidents, as indicated in Table 7, shall result in a Modified System Incident Audit, as defined in Section 5.2.4, Modified System Incident Audit.

Table 7 - Incident Response Criteria and Reporting Requirements

A.	SESSION ACTIVITIES	AUDITABLE	INCIDENT	REPORTABLE
1	Login successes and failures.	Yes	No	No
2	Sessions starts and ends.	Yes	No	No
3	Session timeout (e.g. inactive in excess of 30 minutes).	Yes	No	No
4	ERDS payload submittals, retrievals and when applicable, returns (as described in 4.3.1.4.3, Transaction Activities).	Yes	No	No
B.	**SESSION FAILURES**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	If an ERDS transaction is not conducted within a preset timeout limit, the session will be terminated. Criteria for setting the timeout limit shall be established by the County Recorder; however, the maximum preset timeout limit is 30 minutes.	Yes	No	No
2	If an ERDS session is terminated within a preset timeout limit without receiving a logout command, an incident shall be logged by the ERDS Server.	Yes	No	No

C.	UNAUTHORIZED ACTIVITIES (SECTION 4.3.1.4.2)	AUDITABLE	INCIDENT	REPORTABLE
1	Unauthorized access attempts, including, but not limited to: a. Unauthorized users attempting access to, either physical or logical, ERDS storage areas.	Yes	Yes	Only if fraud is suspected
2	Use of expired or revoked credentials.	Yes	Yes	Only if fraud is suspected
D.	**UNAUTHORIZED ACCESS**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	For Type 1 only, privilege elevation (e.g. “Authorized Access” role performing “Secure Access” tasks).	Yes	Yes	Yes
2	For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session.	Yes	Yes	Only if fraud is suspected
3	For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas.	Yes	Yes	If fraud is suspected
E.	**AUTHENTICATION FAILURES**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	If authentication fails, ERDS returns to the login screen and indicates that access is not authorized.	Yes	No	No
2	If an individual fails to authenticate on consecutive login attempts, the ERDS account shall be locked-out and an incident shall be logged by the ERDS Server. Criteria for setting the login failure limit and lock-out duration shall be established by the County Recorder; however, the maximum preset limit is five attempts.	Yes	Yes	Only if intrusion is suspected
F.	**AUTHORIZATION FAILURES**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	If ERDS cannot determine a role for, or assign privileges associated with a role to, an authenticated user, the session shall be terminated and an incident shall be logged by the ERDS Server.	Yes	Yes	No
G.	**ACCOUNTABILITY FAILURES (SECTION 4.3.1.4.4)**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	Auditable events overwrite other logged events.	Yes	Yes	Only if intrusion is suspected
2	Auditable events cannot be logged.	Yes	Yes	No
3	Logs consume 95% or more of the storage space allocated for logging.	Yes	Yes	No
4	Logs cannot be safely stored.	Yes	Yes	No

H.	ADMINISTRATION REQUIREMENTS (SECTION 4.3.1.5)	AUDITABLE	INCIDENT	REPORTABLE
1	ERDS account creation, modification, deletion, suspension, termination, or revocation, whether authorized or not.	Yes	Only if not authorized	Only if fraud is suspected
2	Hardware or software configuration changes.	Yes	Only if not authorized	Only if not authorized
I.	**TRANSACTION ACTIVITIES (SECTION 4.3.1.4.3)**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	Unique name of the ERDS payload. (Note: This unique name is ERDS-design dependent.)	Yes	Only if out of sequence	No
2	Dates and times the ERDS payload was submitted, retrieved and when applicable, returned.	Yes	Only if not current	No
3	Identity of the individual who submitted, retrieved and when applicable, returned the ERDS payload.	Yes	Only if not authorized	No
4	Name of the organization that the individual represented while submitting, retrieving and when applicable, returning the ERDS payload.	Yes	Only if not authorized	No
5	Success or failure of decryption, validation and hash.	Yes	Refer to "Trans-action Failures"	Only if fraud is suspected
J.	**TRANSACTION FAILURES**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	For Type 1 only, a transmission failure shall display a transmission failure message and generate an auditable event log entry. (Section 3.2, ERDS Payload Submission Process, Table 3, Item 12)	Yes	No	No
2	For Type 1 only, a storage failure shall display a storage failure message and generate an auditable event log entry. (Section 3.2, ERDS Payload Submission Process, Table 3, Item 12)	Yes	No	No
3	A decryption failure shall display a decryption failure message and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 15 and Section 4.2.2.1, Payload Confidentiality)	Yes	Yes	Only if fraud is suspected
4	A hash failure shall display a hash failure message and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 16, and Sections 4.2.2.2, Payload Integrity and 4.2.2.3, Payload Authenticity)	Yes	Yes	Only if fraud is suspected
5	A validity check failure shall display error and/or warning messages and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 17 and Section 4.2.1, Data Integrity)	Yes	Yes	Only if fraud is suspected

K.	UNAUTHORIZED TRANSACTIONS	AUDITABLE	INCIDENT	REPORTABLE
1	Type 1 or Type 2 instrument submitted unencrypted. (Section 4.2.2.1, Payload Confidentiality)	Yes	Yes	Yes
2	Type 1 instrument submitted as a Type 2 instrument or vice versa. (Sections 2.3, Type 1 and/or Type 2 Instruments and 3.4, Processing Multiple Transactions)	Yes	Yes	Only if fraud is suspected
3	Type 1 instrument submitted via an Authorized Access ERDS.	Yes	Yes	Only if fraud is suspected
4	Unauthorized components that draw data or images from sources external to the digital electronic record or digitized electronic record. (Sections 4.2.1, Data Integrity)	Yes	Yes	Only if intrusion is suspected
5	Unauthorized transactions submitted via an ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2. (Section 2.3, Type 1 and/or Type 2 Instruments)	Yes	Yes	Only if fraud is suspected
L.	**SERVER EVENTS (SECTION 4.3.2.4)**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	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.	Yes	Yes	Only if intrusion is suspected
2	For Type 1 only, events for which ERDS System Administrators are alerted of possible or actual intrusion.	Yes	Yes	Only if intrusion is suspected
3	For Type 1 only, hardware or software configuration changes.	Yes	Only if not authorized	Only if not authorized
M.	**NETWORK EVENTS (SECTION 4.3.3.4)**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.	Yes	Yes	Only if intrusion is suspected
2	For Type 1 only, events for which an ERDS System Administrator is alerted of possible or actual intrusion.	Yes	Yes	Only if intrusion is suspected
3	Unauthorized changes to the ERDS operational configuration.	Yes	Yes	Yes
N.	**SECURITY EVENTS**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	Inability to obtain and employ up-to-date anti-malware software. (Sections 4.2, Minimum Security Requirements; 4.2.8, Media Security; and 4.3.2.3, Server Hardening)	Yes	No	No

2	Inability to obtain and employ cryptography, including hashing, encryption and decryption. (Sections 4.2.2.2, Payload Integrity and 4.2.3, Cryptographic Key Generation)	Yes	Yes	Yes
3	Inability to obtain and employ the most up-to-date patches and hot-fixes. (Sections 4.2.8, Media Security and 4.3.2.3, Server Hardening)	Yes	No	Only if intrusion is suspected
O.	**OTHER EVENTS**	**AUDITABLE**	**INCIDENT**	**REPORTABLE**
1	Unauthorized access or changes to storage media, and improper sanitization of storage media. (Section 4.2.8, Media Security)	Yes	Yes	Only if compromise is suspected
2	Any other event that compromises the safety or security of an ERDS. (Section 1.1, Overview)	Yes	Yes	Yes

4.6 SUBSTANTIVE MODIFICATIONS

Substantive modifications, as defined in this section, shall result in a Modified System Audit, as defined in Section 5.2.3, Modified System Audit. A substantive modification is defined as any change that affects the functionality of an ERDS. Substantive modifications include, but are not limited to, the following:

1. Changes to source code that lead to new or different functional behaviors.
2. Changes to call signatures in source code interfaces to purchased components.
3. Changes of data structures or structural database objects.
4. Changes that require modification of deployment procedures.
5. A new version of a compiler that requires source code changes in order to compile existing source code error and warning free.
6. Changes to purchased components or components that are part of software libraries.
7. Relocation of an ERDS server to a different network segment.
8. Changing an ERDS server from single-purpose to multi-purpose.
9. Changing an ERDS server from Single-County to Multi-County.
10. Hardware maintenance involving the complete replacement of an ERDS server.
11. Software maintenance releases that correct, perfect, enhance or otherwise affect the functionality of an ERDS.
12. When changing an instrument type.
13. Changing to a return capability.

The term “substantive modification” excludes the following:

1. Day-to-day administration of ERDS accounts, roles or cryptographic keys.
2. Hardware maintenance that does not affect the functionality of an ERDS and does not involve the complete replacement of an ERDS server.
3. The Off-loading of ERDS server logs to long-term storage.
4. Updating anti-malware software with the most up-to-date releases.
5. Updating operating system software with the most up-to-date patches and hot-fixes.
6. Maintaining backups for software and data.
7. The addition and/or deletion of roles, whether or not fingerprinting or notification to the ERDS Program, is required.

5 AUDIT REQUIREMENTS

5.1 NATURE OF ERDS COMPUTER SECURITY AUDITS

The County Recorder shall establish a disciplined and structured process to monitor the effectiveness of the security controls for the ERDS. The primary process for monitoring the effectiveness of security controls shall be a computer security audit a systematic, measurable, technical assessment of how the baseline security requirements required by the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are applied to an ERDS.

The processes and technologies that are employed in an ERDS shall conform to the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Regardless of how an ERDS is implemented, the security and testing requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

Refer to the System Certification Handbook for the submission of an audit report.

5.2 COMPUTER SECURITY AUDITS

A Computer Security Auditor shall conduct a security audit of an ERDS for the purpose of (1) assessing the safety of the system; (2) verifying that the system is secure from vulnerabilities and unauthorized penetration; (3) ensuring ERDS operating procedures are in place, and are being followed; and (4) that an ERDS has no capability to modify, manipulate, insert, or delete information in the public record. While the requirements, standards, and guidelines in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 assure the safety and security of an ERDS, design variations, advances in technology, new threats, and vulnerabilities require a regular and systematic audit program. ERDS security audits shall be conducted in accordance with security checklists selected by the County Recorder and tailored to reflect local conditions. (Refer to Section 4.4, Security Checklists.)

The facility(ies) of a Type 2 only Authorized Submitter is exempt from a physical security audit when the Computer Security Auditor has validated that all the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 have been met, including certification by the County Recorder and the ERDS Program that the method of submission allowed under the system will not permit an Authorized Submitter or its employees and agents, or any third party, to modify, manipulate, insert or delete information in the public record, maintained by the County Recorder, or information in Type 1 documents which are submitted for electronic recording.

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

5.2.1 Initial System Audit

To obtain initial system certification a full system audit is required. "Initial" is defined as the "first time" application for certification of an ERDS for either a Single-County or a Multi-County. This audit shall be performed prior to activating an ERDS for production and operation and shall be completed by a Computer Security Auditor. The initial audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. A successful initial system audit shall be sufficient to meet the first year audit requirement.

An initial system audit report shall include, but is not limited to, all of the following:

1. A Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.
2. Demonstration of the proposed system in its intended production and operational environments. The audit shall show the following:
    a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the ERDS system.
    b. Transmissions only occur between authorized parties.
    c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
    d. Authorized and unauthorized users are limited in terms of roles assigned to operate the ERDS.
    e. Auditable events are logged correctly.
    f. Known vulnerabilities have been eliminated or mitigated.
    g. The ERDS is not susceptible to published exploits.
    h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
    i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.
3. Testing and review shall include all of the following:
    a. A review of the system design that includes all servers, workstations, and network devices employed for, or in support of, the proposed system.
    b. A review of source code, either selected software components or all software.
    c. An inventory of hardware, software and network devices comprising the proposed system.
    d. An inventory of all users and roles authorized to access and operate the proposed system.
    e. A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.
    f. A review of the ERDS operating procedures proposed by the County Recorder.
    g. A review of all security checklists proposed for auditing the ERDS.
    h. A review of contracts with Authorized Submitters.
    i. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.2 Biennial Audit

To meet the ongoing oversight of an existing certified Single-County ERDS or a Multi-County ERDS, a biennial audit and a local inspection is required in alternating years. The biennial audit is a full system audit that shall be performed in the production and operational environments 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 inspection thereafter by an ERDS Program representative. The biennial audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. Local inspection procedures are detailed in the System Certification Handbook.

A biennial audit report shall include, but is not limited to, all of the following:

1. Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.
2. Demonstration of the ERDS in its production and operational environments. The audit shall show the following:
    a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.
    b. Transmissions only occur between authorized parties.
    c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
    d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.
    e. Auditable events are logged correctly.
    f. Known vulnerabilities have been eliminated or mitigated.
    g. The ERDS is not susceptible to published exploits and that published updates to the standards and guidelines as described in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be implemented within two years.
    h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
    i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.
3. Testing and review shall include all of the following:
    a. A review of the system design that includes all servers, workstations, and network devices employed for, or in support of, the system.
    b. A review of source code, either selected software components or all software.
    c. An inventory of hardware, software and network devices comprising the system.
    d. An inventory of all users and roles authorized to access and operate the system.
    e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.
    f. A review of the ERDS operating procedures established by the County Recorder.
    g. A review of all security checklists established for auditing the ERDS.
    h. A review of contracts with Authorized Submitters.
    i. A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.
    j. A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.3 Modified System Audit

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. The definition of a substantive modification is detailed in Section 4.6, Substantive Modifications. 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, 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 # ERDS0013). The modified system audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. 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:

1. A Description of Deposit Materials showing that modified source code has been deposited in escrow with an approved escrow facility.
2. Demonstration of the ERDS in its intended production and operational environments. The audit shall focus on functions of the substantive modification and show the following:
    a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.
    b. Transmissions only occur between authorized parties.
    c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
    d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.
    e. Auditable events are logged correctly.
    f. Known vulnerabilities have been eliminated or mitigated.
    g. The ERDS is not susceptible to published exploits.
    h. The ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
    i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.
3. Testing and review shall include all of the following:
    a. A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the proposed system.
    b. A review of source code, either selected software components or all software.

c. An inventory of hardware, software and network devices comprising the proposed system.

d. An inventory of all users and roles authorized to access and operate the system.

e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.

f. A review of the ERDS operating procedures established by the County Recorder.

g. A review of all security checklists established for auditing the ERDS.

h. A review of contracts with Authorized Submitters.

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

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

k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.4 Modified System Incident Audit

A Modified System Incident Audit is required to meet the audit requirement resulting from an incident that compromises the safety or security of an ERDS. The definition of an incident is detailed in Section 4.5.2, Incident Response Procedures. A modified system incident audit shall pertain to only the components that were found to compromise the production environment and shall be performed prior to activating the correction in the ERDS for production and operation. This modified system incident audit shall be completed by a Computer Security Auditor and submitted to the County Recorder. The County Recorder shall submit a copy of the successful modified system incident audit report to the ERDS Program. The modified system incident audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. A successful modified system incident audit may not replace the biennial audit requirement.

A modified system incident audit report shall include, but is not limited to, all of the following:

1. Demonstration of the ERDS in its intended production and operational environments. The audit shall focus on the cause of the incident of fraud and show the following:
   a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.
   b. Transmissions only occur between authorized parties.
   c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
   d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.
   e. Auditable events are logged correctly.
   f. Known vulnerabilities have been eliminated or mitigated.
   g. The ERDS is not susceptible to published exploits and that the published updates to the standards and guidelines as described in the ERDS regulations shall be implemented within two years.

h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

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

2. Testing and review shall include all of the following:

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

   b. A review of source code, either selected software components or all software.

   c. An inventory of hardware, software and network devices comprising the system.

   d. An inventory of all users and roles authorized to access and operate the system.

   e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.

   f. A review of the ERDS operating procedures established by the County Recorder.

   g. A review of all security checklists established for auditing the ERDS.

   h. A review of contracts with Authorized Submitters.

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

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

   k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.5 Audit and Local Inspection Schedule

The audit schedule is as follows:

- Year 1 – Initial System Audit
- Year 2 – Local Inspection
- Year 3 – Biennial Security Audit
- Year 4 – Local Inspection if selected
- Subsequent years – alternate Biennial Audit and Local Inspection

5.3 SECURITY AUDIT REPORT FORMAT

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

1. A summary of recommendations in a task-list format.
2. A description of the Computer Security Auditor's methodology.
3. A section for detailed technical observation and recommendation.
4. A diagram depicting results, where applicable.
5. Results of testing and reviews as outlined in Section 5.2, Computer Security Audits.

6. Recommendations for any additional precautions needed to ensure that the system is secure.
7. A copy of the list of all users for secure and/or authorized access.

5.4 PROPRIETARY SOFTWARE

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

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

1. The County Recorder has agreed to allow the Vendor of ERDS Software to include proprietary source code as part of the ERDS.
2. The Vendor of ERDS Software has identified proprietary source code as part of the ERDS.
3. The Computer Security Auditor advises the County Recorder that the safety and security of an ERDS cannot be verified without a source code review.
4. The Computer Security Auditor shall agree to abide by confidentiality requirements of the Vendor of ERDS Software.
5. The Vendor of ERDS Software shall agree that the Computer Security Auditor shall reveal any results of the source code review, conclusions as to the safety and security of an ERDS, findings and recommendations in the audit report.
6. The County Recorder, Computer Security Auditor, and Vendor of ERDS Software shall all agree on methods for including the results, conclusions and recommendations about proprietary source code reviews made by the Computer Security Auditor in the audit report.

6 ESCROW REQUIREMENTS

ERDS source code materials shall be placed into an approved escrow facility when an ERDS is developed for a County Recorder. For each submission, the materials placed in escrow shall be sufficient to maintain the ERDS of every County Recorder that employs those source code materials. This section establishes the escrow requirements to be met.

For the purposes of this section, the phrase “source code materials” includes, but is not limited to, all of the following:

1. A copy of all source code materials that implements an ERDS functionality.
2. A copy of the compiler needed to compile the ERDS source code in escrow.
3. Instructions for installation and use of the ERDS source code compiler.
4. Instructions that facilitate source code reviews, modification and/or recompiling the ERDS source code.

The processes and technologies that are employed in an ERDS shall conform to the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. For the purpose of this section, the term “developer” is defined to mean a Vendor of ERDS Software or public entity that develops software and provides source code materials for an ERDS. Regardless of how an ERDS is implemented, if source code is developed, the escrow requirements outlined in this section shall be met.

6.1 APPROVED ESCROW FACILITY

It is not the intent of the ERDS Program to approve nor certify escrow facilities because this is deemed duplicative of the approval process currently in place by the Secretary of State's office in support of its “escrow of ballot tally software program source codes”. In carrying out its function, the Secretary of State provides a list of facilities approved for use in California on an annual basis, and within ten days of any change affecting the list, to each County Board of Supervisors. In support of protecting ERDS source code, a County Recorder shall select an escrow company from the current Secretary of State's list as obtained from the County's Board of Supervisors.

6.2 LETTER OF DEPOSIT

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

The letter of deposit shall state all of the following:

1. That all source code materials are included in the deposit.
2. The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow.
3. The escrow company, its officers and directors shall not hold or exercise a direct or indirect financial interest(s) in the Vendor of ERDS Software or the County Recorder.

6.3 REQUIREMENTS FOR SUBMISSION

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

6.4 DEPOSIT OF SOFTWARE MODIFICATIONS INTO ESCROW

Substantive modifications, as defined in Section 4.6, Substantive Modifications, shall require updates to source code materials in escrow. Prior to being used to deliver a Type 1 and/or Type 2 instrument in an ERDS, all source code changes or modifications shall be submitted into escrow in the same manner and under the same conditions in which the source code materials were originally placed in escrow.

6.5 INTEGRITY OF MATERIALS

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

6.6 RETENTION AND DISPOSITION OF MATERIALS

Records maintained by the escrow company pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and other applicable law, shall be retained for the term of the escrow agreement. The escrow agreement shall provide for the disposition of source code materials in the event the escrow agreement terminates.

6.7 ACCESS TO MATERIALS

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

6.8 STATE NOT LIABLE FOR ANY COSTS OR ANY OTHER'S ACTIONS

Neither the Attorney General nor the State of California shall be responsible for the fees claimed by the Vendor of ERDS Software, County Recorder or escrow company to establish the escrow contract. Further, neither the Attorney General nor the State of California is a party to the agreement and may not incur any liability for the actions of the parties involved in the escrow agreement.

7 ACRONYMS AND DEFINITIONS

This section defines general terms and phrases used in this document as well as other ERDS handbooks.

Acronym, Term or Phrase	Definitions
Agent	A representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter who has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software. (Refer to the definition of "Vendor of ERDS software (or Developer)" within this section.)
Approved Escrow Company	An escrow company approved pursuant to the California Code of Regulations, Title 2, Division 7, Chapter 6, Article 3, D, List of Approved Companies and Facilities, Section 20639.
Attorney General	The Attorney General of the State of California.
Authorized Access	A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.
Authorized Submitter	A party and his/her employees that has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.
CCISDA	California County Information Services Directors Association
CCR	California Code of Regulations
Certificate Authority	A certificate authority that issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.
CFE	Certified Fraud Examiner
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional

Acronym, Term or Phrase	Definitions
Computer Security Auditor	(1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vender of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.
County Recorder	A public official responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.
County Recorder Designee	A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.
Developer	Refer to Vendor of ERDS Software.
Digital Electronic Record	A record containing information that is created, generated, sent, communicated, received or stored by electronic means, but not created in original paper form.
Digital Signature	A set of electronic symbols attached to, included in, or logically associated with one or more Type 1 and/or Type 2 instruments, inclusive of information related to and intended for association with the Type 1 and/or Type 2 instruments, that is the result of a process, or processes, designed and employed for the purpose of verifying the integrity, accuracy or authenticity of the Type 1 and/or Type 2 instruments with related information. For the purpose of an ERDS, a digital signature is generated by encrypting the hash value of an ERDS payload.
Digitized Electronic Record	A scanned image of the original paper document.
DOJ	The California Department of Justice
Electronic Signature of the Notary	A field or set of fields, containing information about the electronic signature of the notary who notarized a Type 1 or Type 2 instrument.
ERDA	Electronic Recording Delivery Act of 2004.
ERDS	Electronic Recording Delivery System – An ERDS Program certified system to deliver digitized Type 1 and/or Type 2 instruments to a County Recorder, and, when applicable, return to the Authorized Submitter.

Acronym, Term or Phrase	Definitions
ERDS Account Administrator	A secure access role assigned by the County Recorder to an individual authorized to configure accounts, assign roles and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.
ERDS Payload	An electronic structure designed for the purpose of delivering Type 1 or Type 2 instruments to a County Recorder via an ERDS. The structure is also used to return, and, when applicable, Type 1 or Type 2 instruments to an Authorized Submitter via an ERDS.
ERDS Program	The program within DOJ designated by the Attorney General to certify, implement, regulate and monitor an ERDS.
ERDS Server	Computer hardware, software and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the application software associated with an ERDS. The ERDS Server includes software for encrypting, decrypting, hashing, submitting, and, when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.
ERDS System Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.
FIPS	Federal Information Processing Standard
GIAC	Global Information Assurance Certification
GSNA	GIAC Systems and Network Auditor
HMAC	Hash Message Authentication Code
Incident	An event that may have compromised the safety or security of an ERDS.
Instrument	A “Type 1” instrument is defined to mean an instrument affecting a right, title or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. Individuals given role-based privileges for a Type 1 instrument shall be fingerprinted. A “Type 2” instrument is defined to mean an instrument of reconveyance, substitution of trustee or assignment of deed of trust. Type 2 instruments may be delivered as digitized electronic records or digital electronic records. Individuals given role-based privileges for a Type 2 only instrument shall not be fingerprinted.
Lead County	The County Recorder in a Multi-County ERDS responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.

Acronym, Term or Phrase	Definitions
Live Scan	A DOJ system used for the electronic submission of applicant fingerprints. This system is outside of the ERDS Program.
Logged	An auditable ERDS event.
Logical	The way data or systems are organized. For example, a logical description of a file is that it is a collection of data stored together.
MAC	Message Authentication Codes
Multi-County	An ERDS application where County Recorders collaborate and make use of a single ERDS serving multiple counties.
NIST	National Institute of Standards and Technology
Non-Substantive Modification	A change that does not affect the functionality of an ERDS.
ORI	Originating Agency Identifier
Physical Access	Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.
Public Entity	Includes the State, the Regents of the University of California, a county, city, district, public authority, public agency, any other political subdivision or public corporation in the State and federal government entities.
PKI	A Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority, which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with.
Reportable	An incident that has resulted in the compromise of the safety or the security of an ERDS and shall be reported to the ERDS Program.
RSA	A public-key encryption technology developed by Rivest, Shamir and Adelman (RSA). The RSA algorithm has become the de facto standard for industrial-strength encryption especially for data sent over the Internet.
Role	A security mechanism, method, process or procedure that defines specific privileges controlling the level of access to an ERDS.
SANS Institute	Systems and Network Security Institute

Acronym, Term or Phrase	Definitions
Secure Access	A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator authorized to configure hardware, software and network settings; 4) an ERDS Account Administrator authorized to configure accounts, assign roles and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return submitted ERDS payloads.
Security Testing	An independent security audit by a Computer Security Auditor, including, but not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.
SHA	Secure Hash Algorithm
Source Code	A program or set of programs, readable and maintainable by humans, translated or interpreted into a form that an ERDS can execute.
Source Code Materials	Source Code Materials must include, but, are not limited to: 1) a copy of all source code that implements ERDS functionality; 2) a copy of the compiler needed to compile the ERDS source code in escrow; 3) instructions for installation and use of the ERDS source code compiler; and 4) instructions that facilitate reviews, modification and/or recompiling the source code.
Sub-County	The collaborating County Recorder(s) in a Multi-County ERDS operation.
Substantive Modification	A change that affects the functionality of an ERDS.
TLS	Transport Layer Security (formerly known as Secure Socket Layer)
Uniform Index Information	Information collected by a County Recorder in the recording process. Every Type 1 and Type 2 Instruments delivered through an ERDS shall be capable of including uniform index information. The County Recorder shall decide on the content of uniform index information.
User	A person who uses a computer to access, submit, retrieve, or, when applicable, return an ERDS payload.
Vendor of ERDS Software (or Developer)	A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resources used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.
Workstation	A computer used to connect to and interact with an ERDS.

8 REQUIREMENTS MATRIX

The ERDS Program has provided a spreadsheet that illustrates the minimum requirements for each type of ERDS (Type 1 or Type 2 or Type 1 and 2). The Requirements Matrix is an abstracted version of this document so that the minimum requirements are easily referenced. To obtain a copy of the matrix, download it from the ERDS Program web page at http://ag.ca.gov/erds1 or contact the ERDS Program.

8.1 HOW TO READ THE MATRIX

The contents of this document were converted to a Requirements Matrix in order to highlight specific requirements within this document. The column labeled “Title or Requirement” in the Requirements Matrix identifies the actual requirement, whereas the columns labeled “Type 1”, “Type 2” are designated with an “X” to signify which type of ERDS the requirement corresponds to. Only those columns with an “X” in Type 1, or Type 2 are requirements for Type 1, or Type 2 ERDS respectively.

.