

## DOCKETED

<b>Docket Number:</b>	17-BSTD-01
<b>Project Title:</b>	2019 Building Energy Efficiency Standards PreRulemaking
<b>TN #:</b>	221268
<b>Document Title:</b>	Draft 2019 Standards Joint Appendix 7
<b>Description:</b>	Draft version of Joint Appendix 7 for the 2019 Standards update.
<b>Filer:</b>	Adrian Ownby
<b>Organization:</b>	California Energy Commission
<b>Submitter Role:</b>	Commission Staff
<b>Submission Date:</b>	9/20/2017 4:03:55 PM
<b>Docketed Date:</b>	9/20/2017

# Joint Appendix JA7

## Appendix JA7 – Data Registry Requirements

### Table of Contents

<b>Appendix JA7 – Data Registry Requirements .....</b>	<b>1</b>
JA7.1 Purpose and Scope .....	3
JA7.2 Definitions .....	4
JA7.3 Introduction .....	8
JA7.4 Roles and Responsibilities, and Authorized Users.....	9
JA7.4.1 Registration Provider.....	9
JA7.4.2 Authorized Users.....	9
JA7.4.3 View-Only Authorized User .....	9
JA7.4.4 Documentation Author.....	10
JA7.4.5 Field Technician .....	10
JA7.4.6 Registration Signer (Responsible Person).....	10
JA7.4.7 Enforcement Agency.....	10
JA7.5 Document Registration Requirements.....	12
JA7.5.1 Overview.....	12
JA7.5.2 Document Appending.....	12
JA7.5.3 Data Validation for Compliance Document Registration.....	13
JA7.5.4 Registration Numbering Conventions .....	14
JA7.5.5 Verification of Authenticity of Copies of Registered Documents.....	16
JA7.5.6 Project Document Configuration .....	16
JA7.5.7 Certificate of Compliance Requirements.....	18
JA7.5.8 Certificate of Installation Requirements .....	18
JA7.5.9 Certificate of Verification Requirements.....	19
JA7.5.10 Certificate of Acceptance Requirements.....	20
JA7.6 Electronic and Digital Signature Requirements.....	21
JA7.6.1 Introduction.....	21
JA7.6.2 Overall Description .....	21
JA7.6.3 Specific requirements.....	23
JA7.7 Data Exchange Requirements.....	28
JA7.7.1 Data Exchange Requirements for Document Registration .....	28

---

JA7.8	Data Registry Approval .....	30
JA7.8.1	Overview .....	30
JA7.8.2	Application Checklist.....	30
JA7.8.3	Types of Approval .....	31
JA7.8.4	Rescinding Approval (Deactivation) of Data Registries .....	32
JA7.8.5	Data Registry User Manual.....	33
JA7.9	Approval of Software Used for Data Input to Data Registries.....	34
JA7.9.1	Overview .....	35
JA7.9.2	Application Checklist.....	35
JA7.9.3	Types of Approval .....	35
JA7.9.4	Rescinding Approval (Deactivation) of Software .....	36
JA7.9.5	Software User Manual .....	38
JA7.10	Related Publications .....	38

**JA7.1 Purpose and Scope**

Joint Appendix JA7 specifies required functional and technical elements for Data Registries that provide services to authorized users and receive data to produce, register, retain, and distribute copies of compliance documents required for compliance with Title 24, Part 6. The functional and technical elements specified in this document include the following:

- (a) Document registration is defined.
- (b) Roles and responsibilities for users and administrators of data registries are defined.
- (c) Requirements for registered documents are defined.
- (d) Requirements for configuration of project documents in the Data Registry are defined.
- (e) Requirements for electronic and digital signatures used on registered documents are defined.
- (f) Requirements for data exchange between Data Registries and external software tools are defined.
- (g) Requirements for transmittal of copies of documents to a document repository at time of registration are defined.
- (h) Procedures for approval of Data Registries and software used for data input to data registries are defined.

A Data Registry Requirements Manual is expected to be approved by the Energy Commission to provide additional detailed guidance regarding functional and technical aspects of the requirements in Reference Joint Appendix JA7.

## **JA7.2 Definitions**

For the purposes of the specifications in Reference Joint Appendix JA7, the following definitions shall apply:

**Asymmetric Key Encryption** is also known as public key encryption. This type of encryption uses a pair of keys that are mathematically related: one key for encryption and another key for decryption. In digital signature processing, a user is assigned a private key that is not shared with anyone, and a public key that is given to anyone who receives digitally signed material from the user.

From California Code of Regulations, Title 2. Administration, Division 7. Secretary Of State Chapter 10. Digital Signatures, 22003, List of Acceptable Technologies: "The technology known as Public Key Cryptography is an acceptable technology for use by public entities in California..."

All major development environments such as Microsoft and Adobe support PKCS1 asymmetrical key encryption.

**Authorized User** is a person who has a user account with a Data Registry and is required to provide their correct user name and password in order to access the Data Registry. Data Registry users may be required to provide professional licensure, certification or credential information, or other qualifying information as condition of receiving authority to provide signatures for certain types of documentation.

**Commission** means the State of California Energy Resources Conservation and Development Commission, commonly known as the California Energy Commission, also referred to as the Energy Commission.

**Commission Compliance Document Repository** (also known as an electronic document repository) is an electronic database and document storage software application used for retention of Registered electronic Compliance Documents generated by Data Registries, and may also contain data and documentation relevant to other regulatory procedures administered by the California Energy Commission. The Commission Compliance Document Repository shall maintain these retained documents in accordance with Evidence Code section 1530-1532 (in the custody of a public entity).

**Compliance Data Exchange File** is an XML file that contains compliance data used to populate a Compliance Document. The Compliance Data Exchange File is part of the Compliance Registration Package.

**Compliance Document** is one of the following documents required for demonstration of compliance with Title 24, Part 6: Certificate of Compliance, Certificate of Installation, Certificate of Acceptance, Certificate of Verification.

**Compliance Registration Package** means encrypted digital data that is transmitted to a Data Registry that contains the data required for registering a Compliance Document with a Data Registry, including the Compliance Data Exchange File. The most commonly used method is the Zip file format, a data compression and archiving specification that is in the public domain. Files transmitted to a Data Registry using the Zip file format shall be password protected as described in JA7.6.3.2.7.

**Compliance Report Generator** is a web service maintained by the Commission that receives standardized document data exchange files from third party software approved by the Commission and produces the document registration package required to complete registered compliance documents in data registries that are approved by the Commission.

**Compliance Software** is software approved by the California Energy Commission for use in demonstrating compliance with the performance standards in Title 24 Part 6.

**Cryptographic Hash Function** is a mathematical function that creates a unique number that represents the contents of a block of data or text. In digital signature processing the data or text that the user is digitally signing is called the message. The number generated by the cryptographic hash function is called the message digest. To verify a copy of the message, the cryptographic hash function is applied to both the original message and the copy of the message, and the resulting message digests are compared. If they are both the same, then the copy is valid.

There is a number of cryptographic hash functions used in digital signature processing. All major development environments such as Microsoft and Adobe support the most commonly used hash algorithm family, SHA-1, SHA-256, SHA-384, SHA-512 hash algorithms which were developed by National Security Agency (NSA).

**Data Registry** is a web service with a user interface and database maintained by a Registration Provider that complies with the applicable requirements in Reference Joint Appendix JA7, with guidance from the Data Registry Requirements Manual, and provides for registration of residential or nonresidential compliance documentation used for demonstrating compliance with Part 6.

**Residential Data Registry** is a Data Registry that is maintained by a HERS Provider, that provides for registration, when required by Part 6, of all residential compliance documentation and the nonresidential Certificate of Verification.

**Nonresidential Data Registry** is a Data Registry that is maintained by a Registration Provider approved by the Commission, that provides for registration, when required by Part 6, of all nonresidential compliance documentation. However, nonresidential data registries may not provide for registration of nonresidential Certificates of Verification.

**Data Registry Requirements Manual** is a document that provides additional detailed guidance regarding the functional and technical aspects of the Data Registry requirements given in Joint Appendix JA7.

**Digital Certificate** is a computer-based record that contains a person's identifying information and the person's digital signature public key, as well as information about the certificate authority that issued the Digital Certificate and the certificate authority's digital signature verifying the authenticity of the person's identity and digital signature. Although the Secretary of State Digital Signature regulations, Section 22003 (a) 2C states "although not all digitally signed communications will require the signer to obtain a certificate, the signer is capable of being issued a certificate to certify that he or she controls the key pair used to create the signature."

**Digital Signature** an electronic signature that incorporates cryptographic methods of originator authentication, allowing the identity of the signer and the integrity of the data to be verified. The regulations adopted by the Secretary of State that govern the use of Digital Signatures for use by public entities in California are found in the California Code of Regulations, Title 2, Division 7, Chapter 10 Digital Signatures.

**DOCUMENTATION AUTHOR** is a person who prepares a Title 24 Part 6 compliance document that must subsequently be reviewed and signed by a responsible person in order to certify compliance with Part 6.

**Electronic Signature** is a "computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." US 21 Code of Federal Regulations (CFR) Section 11.3.

For the purposes of using electronic signatures to sign compliance documents, the electronic signature shall be an electronic image of the signer's handwritten signature.

**Executive Director** means the Executive Director of the Energy Commission.

**Field Technician** is a person who performs acceptance tests in accordance with the specifications in Reference Joint Appendix NA7, and reports the results of the acceptance tests on the Certificate of Acceptance in accordance with the requirements of Section 10-103(a)4.

**HERS** is the California Home Energy Rating System as described in TITLE 20, Chapter 4, Article 8, Section 1670.

**HERS Provider** is an organization that administers a home energy rating system as described in TITLE 20, Chapter 4, Article 8, Section 1670.

**HERS Rater** is a person who has been trained, tested, and certified by a HERS Provider to perform the field verification and diagnostic testing required for demonstrating compliance with the Part 6, as described in TITLE 20, Chapter 4, Article 8, Section 1670(i).

**HERS Provider Data Registry** is a Data Registry maintained by a HERS Provider.

**Login** (see Secure Login).

**Message** is a block of data or text that has been digitally signed.

**Message Digest** is the unique number generated when a Cryptographic Hash Function is applied to the Message which is the data or text that is digitally signed.

**Password** is a string of characters used for authenticating a user on a computer system.

**Private Key** is one of the keys in Asymmetric Key Encryption used in a Digital Signature. As its name implies, the Private Key should only be known to the owner of the Digital Signature. The private key is used to encrypt the Message Digest of the message that the user digitally signed.

**Public Key** is one of the keys in Asymmetric Key Encryption used in a Digital Signature. As its name implies, the Public Key must be made public to receivers of digitally signed documents in order to decrypt the Message Digest.

**Registered Document** is a compliance document that has been submitted to a residential or nonresidential Data Registry for retention, verified as complete, and has gone through the registration process so that the Registered Document displays all applicable electronic signatures as well as the Registration Provider's digital certificate and the document's unique registration number. The image of the registered document is accessible for printing or viewing by authorized users of the Data Registry via the Registration Provider's internet website. The registered document's unique visible registration number is appended onto the document image by the Data Registry.

A Registered Document meets all applicable requirements in Standards Section 10-103(a), Reference Joint Appendix JA7, and may conform to the guidance given in the Data Registry Requirements Manual.

**Registration** is the process applicable to electronic Compliance Documents that are verified as complete by the Data Registry, and are electronically signed by all required Data Registry Authorized Users. Registration is initiated when an authorized Registration Signer signs the Compliance Document electronically where subsequently the Data Registry adds the Registration Signer's Electronic Signature to the signature block, appends a unique Registration Number to each page of the document, and then applies the Registration Provider's Digital certificate issued by a Certificate Authority approved by the California Secretary of State to the Compliance Document and displays the Registration Provider's digital signature in the signature block. When Registration is complete, the Data Registry immediately and automatically transmits a copy of the completed Registered Compliance Document to the Commission Compliance Document Repository and also retains a copy of the Registered Compliance Document for use by authorized users for submittals.

**Registration Number** is an alphanumeric sequence of digits and delimiters appended to a Compliance Document when the document's Registration Signer provides his or her Electronic Signature to the Data Registry to complete Registration for any document. Each Registration Number shall be unique to only one document. The registration numbering convention utilizes specific digits to reference the document type, revision level, and the parent-child relationships between the compliance documents in a specific project.

**Registration Provider** is an organization that administers a Data Registry service that conforms to the requirements in Reference Joint Appendix JA7 and may conform to the guidance given in the Data Registry Requirements Manual.

**Registration Signer** is a Responsible Person as defined in Title 24, Part 1, Sections 10-103(a)1, 10-103(a)3, 10-103(a)4, or 10-103(a)5 who has established a user account with a Data Registry and has provided sufficient evidence to the Registration Provider to qualify for the authorization to register applicable compliance documentation by providing an electronic signature. The Documentation Author or Field Technician, and Registration Signer on a compliance document may be one and the same person or they may be different persons.

**Secure Login** means the unique Username and Password given to an Authorized User for maintaining the security of the Data Registry.

**Standards** means the California Building Energy Efficiency Standards, Title 24, Part 6.

**Standards Data Dictionary (SDD)** is a dictionary that contains all data and technical terms used to describe building components, equipment, attributes and measurements that are regulated by the

**Standards.** The purpose of the SDD is to provide the vocabulary that is used in expressing standards as well as published compliance documentation.

**URI** stands for Uniform Resource Indicator which is a standard for identifying a name or a resource on the Internet.

**URL** stands for Uniform Resource Locator is a type of URI used to identify locations on the World Wide Web

**Username** is a name that uniquely identifies someone on a computer system. The Username is paired with a Password to create a Secure Login.

**W3C** stands for World Wide Web Consortium which is an international standards body that develops standards for the World Wide Web.

**XML** stands for Extensible Markup Language and is a set of rules for encoding documents in machine-readable form to facilitate the electronic transmission of documents. XML standard was developed by the W3C

**XML Schema refers to XML Schema Definition Language**, commonly referred to as XSD, which is another standard defined by the W3C. An XML schema uses XSD to define a set of rules to which an XML document must conform in order to be considered valid according to that schema. The rules can include definition of major organizational units, definition of data elements and attributes data types, constraints on valid values such as upper and lower bounds, and whether data is required or optional.

**XSL-FO** stands for Extensible Stylesheet Language Formatting Objects and is a standard of the W3C for representing content from an XML document. It is based on a standard vocabulary of document plus formatting and layout directives that can be interpreted by a computer application called an FO processor. XSL-FO is commonly used as a intermediary to generate PDF and printable documents.

**XSLT** stands for Extensible Stylesheet Language Transformation which is a standard from the W3C for translating an XML document into another format such as XSL-FO or HTML.



**JA7.3 Introduction**

A Data Registry is a web service with a user interface and database maintained by a Registration Provider that provides for registration of residential or nonresidential compliance documentation used for demonstrating compliance with Part 6. Data Registries shall conform to the requirements specified in Reference Joint Appendix JA7 and may conform to the guidance given in the Data Registry Requirements Manual.

A Data Registry shall include the minimum functional features specified by Reference Joint Appendix JA7. Additional guidance on functional features may be given in the Data Registry Requirements Manual.

Document registration is the process for verifying, serializing, and signing electronic compliance documents produced using a method approved by the Commission. Approved Data Registries are the entities that implement and manage the procedures for registering documents. The procedures include authenticating and approving users to submit or sign electronic documents and data for registration, validating that these data and documents are completed in conformance with the requirements defined by the Standard Section 10-103(a) and Reference Joint Appendix JA7, and affixing the electronic signature of the Documentation Author. The registration process is completed only when an authorized registration signer signs the compliance document electronically; whereupon the Data Registry automatically performs the following actions:

- (a) Adds the registration signer's electronic signature to the document's signature block.
- (b) Appends a unique registration number to each page of the document.
- (c) Applies the Registration Provider's digital certificate containing their digital signature to the entire compliance document.
- (d) Displays the Registration Provider's digital signature in the signature block that includes a date and time stamp corresponding to the date and time of the document registration process conclusion.
- (e) When the document registration process has concluded, the Data Registry shall immediately and automatically transmit a copy of the completed registered compliance document to the Commission Compliance Document Repository.
- (f) The Data Registry shall also retain a copy of the registered compliance document for use by authorized users for submittals.

Paper copies of registered compliance documents printed directly from the Data Registry website, or electronic copies downloaded from the Data Registry website shall be used for submittal to enforcement agencies or other parties to the building construction project.

The Registration Provider's digital signature provides for automatic electronic verification of the authenticity of electronic copies of registered documents.

The electronic copies of the registered documents retained by the Commission Compliance Document Repository shall be utilized to satisfy public information requests, perform research, and shall be maintained in a manner conforming to Evidence Code section 1530-1532 (in the custody of a public entity) for use in enforcement of the Standards.

Any person or entity wishing to have a Data Registry approved shall submit an application to the Energy Commission. Data Registries may be approved by the Energy Commission or by the Executive Director to provide document Registration services. Data Registries shall conform to the requirements of Reference Joint Appendix JA7. Detailed guidance for implementation of the requirements in Appendix JA7 may be given in the Registry Requirements Reference Manual.

---

## **JA7.4 Roles and Responsibilities, and Authorized Users**

This section summarizes the roles and responsibilities for the individuals who participate in the document registration procedures administered by a Data Registry. However, this section is not a complete accounting of the responsibilities of the respective parties.

### JA7.4.1 Registration Provider

A Registration Provider is an entity that has been approved by the Energy Commission to provide Data Registry services. Registration Providers maintain Data Registries that conform to the requirements in Reference Joint Appendix JA7 and utilize the guidance in the Data Registry Requirements Manual. Registration Providers are required to retain completed registered compliance documents and make copies of the registered documents available to authorized users for submittals to enforcement agencies or to other parties to the building project that require the documents. Registration Providers make services available that enable authorized users of their Data Registry to verify the authenticity of paper and electronic copies of the retained registered documents.

In order to facilitate Commission oversight of a Registration Provider's documentation processes, the Registration Providers shall grant authorization to Energy Commission staff to view the data and documents retained in the Data Registry, and shall provide functionality that allows Energy Commission staff to query retained data or documents. For residential compliance document registration, the Registration Provider is required to be a HERS Provider approved by the Energy Commission. For nonresidential compliance document registration, the Registration Provider is required to be a Registration Provider approved by the Commission.

### JA7.4.2 Authorized Users

Authorized users are persons who have established a user account with a Data Registry and are required to provide their correct user name and password in order to access the secured information in that Data Registry. Data Registry authorized users may be required to provide proof of professional licensure, professional certification, or other qualifying information as a condition for receiving authority to access records or provide signatures for certain types of documentation. User accounts shall be established for each Data Registry for which a user must gain access.

The information required to establish a user account with a Data Registry shall be determined by the Registration Provider who shall gather and verify any and all information necessary to validate a user applicant's identity or applicable professional qualifications as prerequisite to authorizing assignment to a user applicant an electronic signature, or permissions as a documentation author, or permissions as a registration signer.

Authorized Users may not share their Secure Login with any other individual for any purpose. Violation of this policy may constitute fraud, and can be cited as a reason for denial of access for all the persons involved, including the user who releases their Secure Login to another person or persons, and the person or persons who use the Secure Login to gain access the Data Registry.

Additional guidance for establishing user accounts may be given in the Data Registry Requirements Manual.

The roles and responsibilities in the remainder of this section JA7.4 describe specific types of authorized users of the Data Registry. Additional guidance describing roles and responsibilities of Registration Providers and authorized users may be described in the Data Registry Requirements Manual.

### JA7.4.3 View-Only Authorized User

Data Registries may provide user accounts that allow users to view only certain records. These types of accounts may allow access to records to view, print or download copies of compliance documents in order to validate the information submitted to enforcement agencies on paper copies of registered documents, and for determining the status of completion of the full documentation package for a project.

#### JA7.4.4 Documentation Author

Documentation Authors are persons who prepare Title 24 Part 6 compliance documents that must subsequently be reviewed and signed by a Registration Signer (responsible person) in order to certify compliance with Part 6.

Documentation Authors assist with input of information required to complete the compliance documents required for the registration procedures in a Data Registry. Documentation authors who provide support for preparation of compliance documents in a Data Registry shall establish a user account and an electronic signature authority with the Data Registry. Documentation Authors shall sign the documents they prepare, but documentation author signatures do not indicate or assume responsibility for the truth or validity of the information reported on a compliance document. Documentation Authors may engage in business relationships with the Registration Signers they assist, or they may be employees of the Registration Signers they assist.

#### JA7.4.5 Field Technician

The Field Technician is responsible for performing the acceptance test procedures and documenting the results of the acceptance tests on a Certificate of Acceptance. The Field Technician shall sign the Certificate of Acceptance to certify that the information he reports on the Certificate of Acceptance is true and correct. When registration of a Certificate of Acceptance is required, the Field Technician shall establish a user account and an electronic signature authority with the Data Registry in order to provide electronic signatures to complete the Certificate of Acceptance. When a Field Technician also performs the data input to prepare the Certificate of Acceptance documentation, the Field Technician shall also provide the documentation author signature on the Certificate of Acceptance. The Field Technician may be, but is not required to be the installer of the system that requires Acceptance Testing.

#### JA7.4.6 Registration Signer (Responsible Person)

The Registration Signer is the person responsible for the work identified on a compliance document (Certificate of Compliance, Certificate of Installation, Certificate of Acceptance, or Certificate of Verification).

- (a) **For Certificate of Compliance documentation**, the Registration Signer shall be eligible under Division 3 of the Business and Professions Code to accept responsibility for the building design.
- (b) **For Certificate of Installation documentation**, the Registration Signer shall be eligible under Division 3 of the Business and Professions Code to accept responsibility for the building construction or installation in the applicable classification for the scope of work identified on the document.
- (c) **For Certificate of Acceptance documentation**, the Registration Signer shall be eligible under Division 3 of the Business and Professions Code to accept responsibility for the system design, construction or installation in the applicable classification for the scope of work identified on the document.
- (d) **For Certificate of Verification documentation**, the Registration Signer shall be a certified HERS Rater.

The Registration Signer shall provide a signature to certify that the information reported on a compliance document for which he is responsible is true and correct. When registration of a compliance document is required, the Registration Signer shall establish a user account and an electronic signature authority with the Data Registry. When a Registration Signer also performs the data input to prepare a compliance document, the Registration Signer shall also provide the documentation author signature on the compliance document.

#### JA7.4.7 Enforcement Agency

Standards Section 10-103(d) requires the Enforcement Agency to verify that all required compliance documents for a project are completed, signed, and submitted or posted as required by Standards Section 10-103(a). Thus, when Section 10-103(a) requires that a compliance document be registered with a Data

Registry, the Enforcement Agency must verify that compliance documents submitted when applying for a permit, or posted in the field are registered documents. Such enforcement agency verification shall be by any valid means the Enforcement agency considers satisfactory.

Enforcement Agency persons may establish user accounts with data registries to enable viewing the compliance documents for projects for which their jurisdiction has enforcement authority.

Enforcement Agencies may be authorized to enter notations into project records in data registries to communicate plan check and field inspection information to builders, designers, installers and raters.

## **JA7.5 Document Registration Requirements**

### JA7.5.1 Overview

All compliance documents for which registration is required shall be produced by a method approved by the Commission and then registered with an approved Data Registry by authorized users of the Data Registry. Procedures for submittal of required documentation to enforcement agencies and other parties to the building construction project are given in Reference Residential Appendix RA2, and Reference Nonresidential Appendices NA1. Standards Section 10-103(a) defines the administrative requirements for the compliance documents (Certificate of Compliance, Certificate of Installation, Certificate of Acceptance, and Certificate of Verification).

Compliance document layouts shall be defined by standardized data structures implemented according to the requirements given in JA7.7. Compliance documents produced by the Data Registry shall conform to the applicable informational content and graphical layout formatting approved by the Energy Commission.

The Data Registry shall be capable of tracking all compliance documentation and maintaining the correct associations between related documents within a building project. Any revisions to compliance documents shall be tracked and reported.

The Data Registry shall ensure that registered documents are retained such that they are available to authorized users for submittals to enforcement agencies or other parties to the building construction project that require copies of the registered compliance documents.

Contingent upon the availability of a Commission Compliance Document Repository, the Data Registry shall immediately and automatically, upon concluding the registration of compliance documents, transmit a copy of each registered compliance document to the Commission Compliance Document Repository.

### JA7.5.2 Document Appending

The compliance document informational content, graphical layout, and formatting used by the Data Registry shall conform to the document layouts and data structures approved by the Energy Commission as further described in Section JA7.7. The Data Registry shall be capable of receiving electronic compliance documents and compliance data produced by the methods approved by the Commission, and append the compliance documents received from authorized users according to the requirements in JA7.5.

When data exchange procedures for compliance documents are required, the data definitions and data formatting required by Section JA7.7 shall be used.

Electronic document layouts implemented in Commission-approved methods for producing compliance documents shall include specifications indicating coordinate locations and positions where the Data Registry will affix Registration Signer's Electronic Signatures, registration numbers, registration date and time record information and Data Registry provider logos and watermarks.

The ACM Reference Manual will include additional detailed guidance necessary to assist compliance software tools in providing document output formatted to coordinate with these Data Registry-specific information features.

The following conventions shall be enforced:

#### **JA7.5.2.1 Registration Number**

The registration number for a multiple-page document shall be visible on all pages of the document.

#### **JA7.5.2.2 Registration Date and Time**

The registration date and time shall reflect the point in time corresponding to the submittal of the electronic certification signature by the person responsible for the information on the document. The format for the registration date and time record shall be calendar date (year-month-day) with time of day (hour-minutes-

seconds). Hour of the day shall utilize 24-hour format. Additional guidance describing the formatting and location for these features may be given in the Data Registry Requirements Manual.

### **JA7.5.2.3 Performance Compliance Software Calculation Date and Time**

The performance compliance calculation date and time information that is generated by the compliance software tool shall be retained as data in the record for the registered Certificate of Compliance document in the Data Registry.

The date and time information for the compliance calculation for a multiple-page performance Certificate of Compliance document shall be visible on all pages of the compliance document.

### **JA7.5.2.4 Electronic Signatures**

Registered documents shall be electronically signed by the documentation authors, and by the persons who are eligible to assume responsibility for the documentation as specified by Standards Section 10-103(a) and who are authorized users of the Data Registry who have established an electronic signature authority with the Data Registry. The Registration Provider shall ensure that all required electronic signature features and procedures specified in Section JA7.6 are implemented and enforced. The electronic signature layouts and locations shall be consistent with the document layouts approved by the Energy Commission. Additional guidance on the location and formatting may be given in the Data Registry Requirements Manual.

### **JA7.5.2.5 Digital Signatures**

The Registration Provider shall ensure that the required digital signature procedures specified in Section JA7.6 are enforced. Guidance for the location for the visible aspects of the Registration Provider's digital signature may be described in the Data Registry Requirements Manual.

## **JA7.5.3 Data Validation for Compliance Document Registration**

Data Registries shall have the capability to automatically perform validation of data entered by a documentation author to complete a compliance document as required by the document data validation procedures in Section JA7.6.3.2.2.

There shall be a data validation rule set specific to each compliance document.

Detailed guidance for the data validation rules may be provided in the Data Registry Requirements Manual.

Compliance document data validation rules may be implicit in the formatting of the data elements that define a compliance document for data exchange processes, or data validation rules may be implemented by the Data Registry software.

Data validation rules or specifications may be defined in the XML schema that represents the compliance data for a compliance document as further described in Section JA7.7. Validation criteria such as whether data is required or optional, the required data type, the data numeric upper and lower bounds, acceptable enumeration values, calculations that must be performed, etc., can all be defined in the XSD file.

The Data Registry Requirements Manual will provide guidance for the methods for validation of the data taking into consideration the specifications for the data elements for the data exchange processes described in Section JA7.7.

The Data Registry may flag data entry errors at any time during data entry, however all data validation shall be completed prior to allowing a documentation author signature action to be completed. Documents shall not be marked as ready for registration signing unless all required data validation errors have been corrected, and a documentation author signature action has been completed successfully.

The following conventions shall be enforced as a condition for registration of a document:

**JA7.5.3.1 Null Entries**

When completion of a compliance document requires data entry for an information field, the data shall be entered, otherwise registration shall not be allowed. However, if data entry for a particular information field is optional, a null entry shall not prevent registration from concluding.

**JA7.5.3.2 Calculated Values**

Whenever possible or practical, the Data Registry shall perform the calculations required for determining compliance results. Guidance for calculations may be given in the Data Registry Requirements Manual.

**JA7.5.3.3 Look-up Functions for Calculations**

Whenever possible or practical, the Data Registry shall use lookup functions that provide values needed for completing calculations as referenced from the applicable protocols in the Reference Appendices or from Standards compliance criteria. Guidance for application of lookup functions may be given in the Data Registry Requirements Manual. .

**JA7.5.4 Registration Numbering Conventions**

Registration numbers used for the document registration procedures described in Joint Appendix JA7 are alphanumeric sequences of digits and delimiters that are appended to a compliance document when the document's registration signer performs an electronic signature action in the Data Registry to conclude the registration procedure for a document. Each registration number shall be unique to only one document. The registration numbering convention assigns significance to certain digits in order to define the document type, document revision level, and the parent-child relationships between the compliance documents contained in a project. As the compliance document types required for residential projects are different than those required for nonresidential projects, the numbering conventions used shall conform to the conventions specified in sections JA7.5.4.1 and JA7.5.4.2 respectively.

Registration numbering conventions for other documentation processes are possible. Any new document process for which the Commission requires the documents to be registered shall use a registration numbering convention that is approved by the Commission.

**JA7.5.4.1 Nonresidential Registration Numbering Convention**

Contingent upon approval of nonresidential Data Registries, a nonresidential registration numbering convention shall be determined and approved by the Commission in conjunction with the approval of the first nonresidential Data Registry, and shall be used by all nonresidential data registries thereafter. The nonresidential registration numbering convention specification shall use a similar design concept as used in the residential registration numbering convention specified in Section JA7.5.4.2 which assigns significance to digits in order to define the document type, document revision level, and the relationships between the compliance documents contained in a project.

**JA7.5.4.2 Residential Registration Numbering Convention**

The registration numbers assigned to residential compliance documents by the Data Registry at the conclusion of the registration process shall conform to the conventions described in this section. Refer to Figure JA7.5-1 for information that defines the numbering convention, and an example registration number.

<b>1</b>	<b>1</b>	<b>3</b>	-	<b>N</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>7</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>B</b>	-	<b>M</b>	<b>2</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>5</b>	<b>2</b>	<b>A</b>	-	<b>M</b>	<b>2</b>	<b>1</b>	<b>C</b>
<b>provider</b> (1=CHEERS; 2=CaICERTS; 3=CBPCA; sequential) year digit 3 of 4 (eg 3rd digit of year 2013 is shown in example below) year digit 4 of 4 (eg 4th digit of year 2013 is shown in example below)			-	<b>CC Type</b> (N=new residential, A=alteration residential, D=additional residential) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) Revision Level (alpha only: A=first issuance; then sequential B through Z)								-	<b>CI Type</b> (E=envelope, L=lighting, M=mechanical) CI Type (first numeric digit eg "2" from the mech-21) CI Type (second numeric digit eg "1" from the mech-21) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) numeric (sequential 0 through 9) Revision Level (alpha only: A=first issuance; then sequential B through Z)								-	<b>CV Type</b> (E=envelope, L=lighting, M=mechanical) CV Type (first numeric digit eg "2" from the mech-21) CV Type (second numeric digit eg "1" from the mech-21) Revision Level (alpha only: A=first issuance; then sequential B through Z)				
			-	9,999,999 numbers + 0								-	99,999 numbers								-					
			-	<b>Certificate of Compliance (CC)</b>								-	<b>Certificate of Installation (CI)</b>								-	<b>Certificate of Verification (CV)</b>				
			-	use 000000000 for CC documents								-	use 000000000 for CI documents								-	use 0000 for CC, CI documents				

Use only capitalized alpha digits; Omit use of the letter "O" to avoid confusion with the number Zero "0"; Omit use of the letter "I" to avoid confusion with the number One "1";

Figure JA7.5-1. Residential Registration Numbering Convention (and Example Number)

As shown in Figure JA7.5-1, the significance of the digits provides descriptors for: the Registration Provider; the year; the type of compliance document; relationships between the documents; and the revision level of the respective documents. The digit type (Alpha or Numeric) and sequencing are also given.

The following are examples of registration numbers and the interpretation of the significance of the numbering as consistent with the descriptions given in Figure JA7.5-1.

113-N0007321B-000000000-0000: CHEERS Provider, 2013 year project, residential new construction Certificate of Compliance document type, and sequential number 0007321, revision B.

113-N0007321B-M2100052A-0000: Certificate of Installation document type associated with the above Certificate of Compliance #113-N0007321B-00000000-0000, MECH-21 Certificate of Installation type, and sequential number 00052, revision A.

113-N0007321B-M2100052A-M21C: Certificate of Verification associated with the above Certificate of Installation #113-N0007321B-M2100052A-0000, MECH-21 HERS Certificate of Verification document type, revision C.



### JA7.5.5 Verification of Authenticity of Copies of Registered Documents

For projects for which Standards Section 10-103(a) requires the documents to be registered, compliance requires that documents shall first be registered with a Data Registry before being submitted to an enforcement agency for approval. Additionally, when revisions to the compliance documents are necessary, compliance requires the revised documents to be registered with the Data Registry prior to re-submittal to the enforcement agency for approval. Thus, the current revision of a registered document in the Data Registry shall be the reference document for validation of the authenticity of a document submitted to an enforcement agency or to another party to the construction project.

Registration Providers shall make available document verification services to authorized users of their Data Registry.

Methods for verification of a document's authenticity shall include basic visual comparison of a copy of a registered document to the current version of the registered document on file in the Data Registry.

Additionally, the automated document validation utility that is made possible by digital signature technology makes it possible for a document recipient to automatically verify an electronic copy of a registered compliance document without having to manually inspect it against the registered document in the Data Registry. As described in Section JA7.3, the last step in the document registration procedure in the registry applies the Registration Provider's digital certificate containing their digital signature to the entire compliance document, thus providing the capability for automated verification of authenticity of electronic copies of the registered document.

Additional guidance for use of the Data Registry digital signature technology for verification of document authenticity may be given in the Data Registry Requirements Manual, and in the Residential and Nonresidential Compliance Manuals.

### JA7.5.6 Project Document Configuration

Data Registries shall be capable of tracking all compliance documentation and maintaining the correct associations between related documents, including revisions and completion statuses for all documents within a building project.

A certificate of compliance establishes the requirements for project documentation for prescriptive and performance compliance methods.

2013 Standards introduced mandatory HERS verification for residential projects for which there are options for compliance with the mandatory requirement. Thus, indication of the option selected for compliance with a residential mandatory measure may not be known until after a Certificate of Installation is submitted to a Data Registry to demonstrate compliance with the mandatory requirement. The Data Registry shall track when Certificate of Installation documents are registered for any mandatory measure that has an option for compliance; shall report any HERS verification requirement that is triggered by the mandatory measure; and ensure that any required HERS verification is completed as a condition of compliance. Additional guidance describing residential Data Registry tracking of mandatory measure options and the required documentation for the mandatory options may be provided in the Data Registry Requirements Manual.

#### **JA7.5.6.1 Project Status Reports**

The status of completion of a project shall be reported by the Data Registry.

The Data Registry shall determine the documents required for a project based on the Certificate of Compliance and maintain a summary that reflects the current status of completion of the required documents and shall be readily accessible to authorized users of the Data Registry. Access to the report shall be facilitated by use of search parameters relevant to the project as listed in Sections JA7.5.6.1.1 and JA7.5.6.1.2.

Enforcement Agencies may be authorized to enter notations into project records in data registries to communicate plan check and field inspection information to builders, designers, installers and raters.

The project status report shall be made available in a printable format.

Minimum information requirements for the project status report shall include the following:

**JA7.5.6.1.1 Project Status Report Information for Residential Projects:**

- (a) Project name
- (b) Project location (or address)
- (c) Listing of the Certificate of Compliance documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number
- (d) Listing of the Certificate of Installation documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number
- (e) Listing of the Certificate of Verification documents required; date registered or indicate not complete if the document record has been started but is not yet registered); registration number
- (f) Listing of the mandatory measure options required; options selected (refers to the Certificate of Installation and Certificate of Verification documentation).

**JA7.5.6.1.2 Project Status Report Information for Nonresidential Projects:**

Note: Nonresidential Document registration is contingent upon approval of a nonresidential Data Registry by the Commission, and the requirement for nonresidential document registration is not effective until January 1, 2015.

- (a) Project name
- (b) Project location (or address)
- (c) Listing of the Certificate of Compliance documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number
- (d) Listing of the Certificate of Installation documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number
- (e) Listing of the Certificate of Acceptance documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number
- (f) Listing of the Certificate of Verification documents required; date registered (or indicate not complete if the document record has been started but is not yet registered); registration number.

**JA7.5.6.2 Revision Control**

When a revision to a compliance document is made, the revised version of the compliance document shall also be registered (a registration signer must sign again to register the revision), and the revision digit for the compliance document shall be incremented. Thus a copy of each registered revision of each registered document shall be transmitted to the Commission Compliance Document Repository.

When a revision is made to a compliance document that is associated with one or more registered dependent (child) documents, the dependent documents shall have their registered status revoked, and their status shall be reported as incomplete (orphaned) until signed again by the registration signer subsequent to making any necessary changes to the "orphaned child" document made necessary by the revision of the applicable dominant (parent) document. A new registration signature is required for the orphaned child document in order to update the registration number such that the new revision level of both the parent and the child documents is shown.

A copy of the new revision of a document shall be submitted to the enforcement agency for all applicable approvals or inspections.

The data that was used to create obsolete versions of compliance documents shall not be required to be retained in the Data Registry history or memory. However, a copy of each revision of each registered electronic document shall be retained.

The current revision of any document in the registry shall be considered to be the only valid version of that document. All previous revisions of that document shall be considered obsolete, thus not valid for use for submittal to enforcement agencies to demonstrate compliance.

#### JA7.5.7 Certificate of Compliance Requirements

##### **JA7.5.7.1 Prescriptive Certificate of Compliance Document**

Procedures for submittal of prescriptive Certificate of Compliance documents may be by direct keyed-in data entry as described in Section JA7.7.1.1, or by other methods if approved in accordance with Section JA7.9. Guidance for the procedures and requirements for Data Registry features for prescriptive certificate of compliance document registration may be given in the Data Registry Requirements Manual.

##### **JA7.5.7.2 Performance Certificate of Compliance Document:**

Procedures for submittal of the performance Certificate of Compliance shall use Compliance Software approved by the Commission pursuant to all applicable procedures in Title 24 Part 1, Section 10-109, and shall conform to all applicable data exchange requirements given in Section JA7.7.

##### **JA7.5.7.3 Multiple Orientation Plans (Residential)**

The Data Registry shall ensure that multiple orientation performance Certificate of Compliance documents are configured in the Data Registry such that the registered multiple orientation Certificate of Compliance document is referenced for all build-outs of that master plan. The registered Certificate of Compliance that was approved by the enforcement agency shall be the Certificate of Compliance document that is the parent document for each and every dwelling unit built from that master plan.

Detailed guidance describing the procedures for tracking revisions to multiple orientation Certificate of Compliance Documents may be given in the Data Registry Requirements Manual.

##### **JA7.5.7.4 Multifamily Dwelling units**

The Data Registry shall ensure that multifamily whole-building performance Certificate of Compliance documents are configured in the Data Registry such that the registered multifamily Certificate of Compliance document is referenced for all dwelling units in the multifamily building. The registered Certificate of Compliance that was approved by the enforcement agency shall be the Certificate of Compliance document that is the parent document for each and every dwelling unit specified by that whole-building certificate of Compliance document.

Detailed guidance describing the procedures for tracking revisions to multifamily whole-building Certificate of Compliance Documents may be given in the Data Registry Requirements Manual.

#### JA7.5.8 Certificate of Installation Requirements

##### **JA7.5.8.1 Residential Certificate of Installation**

Procedures for submittal of residential Certificate of Installation documents may be by direct keyed-in data entry as described in Section JA7.7.1.1, or by other methods if approved in accordance with Section JA7.9. Detailed guidance for the functional and technical elements necessary for registration of residential Certificate of Installation for a Data Registry may be given in the Data Registry Requirements Manual.

##### **JA7.5.8.2 Nonresidential Certificate of Installation**

Nonresidential Certificate of Installation document registration is contingent upon the approval of nonresidential Data Registries, and in any event shall not be required before January 01, 2015.

Procedures for submittal of Nonresidential Certificate of Installation documents may be by direct keyed-in data entry as described in Section JA7.7.1.1, or by other methods if approved in accordance with Section JA7.9. Detailed guidance for the functional and technical elements necessary for registration of Nonresidential Certificate of Installation documents for a Data Registry may be given in the Data Registry Requirements Manual.

JA7.5.9 Certificate of Verification Requirements

Certificate of Verification documents are always registered documents.

Procedures for submittal of Certificate of Verification documents may be by direct keyed-in data entry as described in Section JA7.7.1.1, or by other methods if approved in accordance with Section JA7.9. Detailed guidance for the required functional and technical elements necessary for registration of Certificate of Verification documents for a Data Registry may be given in the Data Registry Requirements Manual.

**JA7.5.9.1 Managing Sample Groups**

HERS Provider Data Registries are required to manage the group sampling procedures. Details that describe the requirements for managing sample groups are given in Reference Residential Appendix RA2 and in Reference Nonresidential Appendix NA1.

**JA7.5.9.2 Group Numbering Convention**

Group number is a HERS Provider-designated identification number unique to the sample group to which a dwelling has been assigned. The Providers shall utilize the numbering convention given in Figure JA7.5-2. below. The group number shall be reported on all Certificate of Verification documents that utilize group sampling for compliance.

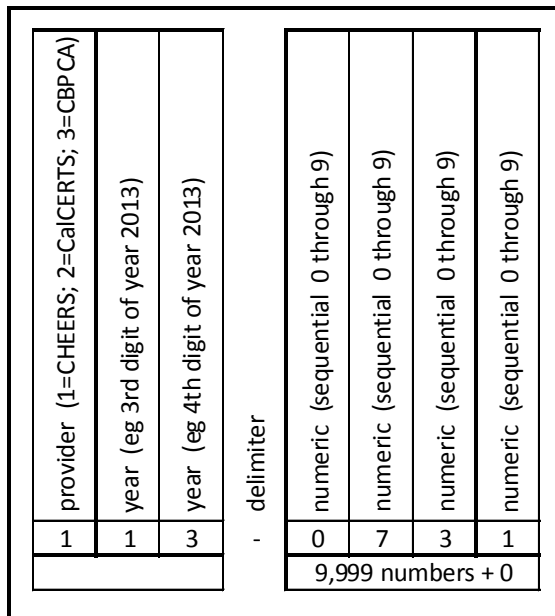


Figure JA7.5-2. Group Numbering Convention (and Example Number)

The following is an example group number and the interpretation of the significance of the numbering consistent with the descriptions given in Figure 4-1.

113-0731: CHEERS, group opened during year 2013, sequential group number 0731

#### JA7.5.10 Certificate of Acceptance Requirements

Certificate Acceptance document registration is contingent on the approval of nonresidential Data Registries, and in any event shall not be required before January 01, 2015.

Procedures for submittal of Certificate Acceptance documents may be by direct keyed-in data entry as described in Section JA7.7.1.1, or by other methods if approved in accordance with Section JA7.9. Detailed guidance for the required functional and technical elements necessary for registration of Certificates of Acceptance documents for a Data Registry may be given in the Data Registry Requirements Manual.

---

## **JA7.6 Electronic and Digital Signature Requirements**

### JA7.6.1 Introduction

This section defines the functional and technical requirements for the use of electronic and digital signatures in the registration of compliance documents. These specifications shall be implemented by a Data Registry as a condition of approval of the Data Registry by the Commission.

### JA7.6.2 Overall Description

#### **JA7.6.2.1 Interfaces - Main Users**

- (a) **Authorized Users** of Data Registries who must sign Compliance Documents either as the Documentation Author, or Field Technician, or as the Registration Signer (responsible person).
- (b) **Registration Providers** who must implement the electronic and digital signature specifications into the Data Registry user interface to provide Electronic Signature capabilities to the Authorized Users of the Data Registry, and must append their digital signature to all registered compliance documents created in their Data Registry.
- (c) **Commission Compliance Document Repository** which must receive registered documents transmitted from the Data Registries and will process the digital signature to validate the sender and the contents.
- (d) **Persons or Software Entities who Validate Electronic Documents** who may receive electronic copies of registered documents made available by the Data Registries and will process the digital signature to validate the sender and the contents.
- (e) **Compliance Software Tools** that export compliance documents for transmittal to the Data Registries that must subsequently be electronically signed and registered in the Data Registry.

#### **JA7.6.2.2 Major Functions**

The electronic and digital signature requirements of the Data Registry consist of the following major functions:

##### **JA7.6.2.2.1 Electronic Signature Capability**

The Data Registry shall provide electronic signature capability to authorized users.

##### **JA7.6.2.2.2 Document Data Validation**

The Data Registry shall check that compliance documents are complete and the data entered meets the data validation rules for the applicable document before making the documents available for signing or registering.

##### **JA7.6.2.2.3 Signer Review and Signature Actions**

The Data Registry shall provide functionality for authorized users to select, review, and sign compliance documents as a Documentation Author, Field Technician, or Registration Signer.

##### **JA7.6.2.2.4 Digital Signatures**

The Data Registry shall apply the Registration Provider's Digital Signature to compliance documents electronically signed by the registration signer when concluding the document registration procedure in the Data Registry, and then append the Registration Provider's digital certificate issued by a certificate authority approved by the California Secretary of State.

The function of the Registration Provider's digital certificate is to provide verification from an approved certificate authority that the document came from the Registration Provider's Data Registry and to provide automated document verification to persons or agencies that receive electronic submittals of these registered documents.

#### **JA7.6.2.2.5 Transmittal to Commission Compliance Document Repository**

The Data Registry, upon completion of the registration procedure, shall immediately and automatically transmit a copy of the completed registered compliance document to the Commission Compliance Document Repository which will process the Registration Provider's digital certificate to validate the sender and the compliance document contents.

#### **JA7.6.2.2.6 Document Retention**

The Data Registry shall retain a copy of the completed registered electronic compliance document and make the document available for use by authorized users of the registry who may access a copy of the registered document and may subsequently process the Registration Provider's digital certificate to verify the sender and the compliance document contents.

#### **JA7.6.2.2.7 Receive and Process Output From Compliance Software and Other Software Tools**

The Data Registry shall process the completed Compliance Registration Package from Compliance software tools or other software tools approved by the Commission for use in the Compliance Document Registration process.

### **JA7.6.2.3 User Characteristics**

There are four categories of users who will participate in the electronic and digital signature functionality:

#### **JA7.6.2.3.1 Users who will use electronic signatures to sign and register compliance documents.**

This is a heterogeneous category composed of HERS Raters, building designers, building contractors, installation contractors, energy consultants, home owners, and others.

#### **JA7.6.2.3.2 Users who use a digital certificate to secure registered compliance documents.**

This category consists of each approved Registration Provider.

#### **JA7.6.2.3.3 Users who will receive the electronically transmitted registered compliance documents**

These users will need to apply decryption processing using the digital certificate to identify the sender and verify the contents of the received document. The Commission Compliance Document Repository is a main user in this category. Also, users who take advantage of digital signature automated verification capabilities to verify the authenticity of registered compliance documents received as electronic submittals from various other participants in the compliance documentation process will be another main user in this category.

#### **JA7.6.2.3.4 Users who transmit electronic compliance documentation to the Data Registry.**

Title 24 compliance software tools are the main users in this Category. The electronic compliance documents exported from the compliance tools must be formatted to provide location coordinate information for use when applying the visible aspects of electronic and digital signatures to the compliance documents. The Data Registry must be capable of appending the visible aspects of electronic and digital signatures to the correct locations in the signature blocks on the imported compliance documents during the subsequent electronic signature and registration procedures.

Detailed guidance for electronic and digital signature target coordinate information may be described in the 2016 Alternative Calculation Method (ACM) Reference Manual to assist in the implementation of the requirements by compliance software vendors. The Data Registry shall implement the capability to append

the visible aspects of electronic and digital signatures to the signature blocks on compliance documents in these locations.

#### **JA7.6.2.4 Constraints**

##### **JA7.6.2.4.1 Schedule Constraint:**

The electronic and digital signature capabilities shall be implemented at least six months before the effective date for the 2016 Standards.

##### **JA7.6.2.4.2 Software Constraint:**

The digital signature technology including the hash algorithm and asymmetric key encryption used shall be consistent across all Data Registries because the Commission Compliance Document Repository will not support multiple approaches.

### JA7.6.3 Specific requirements

#### **JA7.6.3.1 Interface Requirements**

##### **JA7.6.3.1.1 User interfaces**

*JA7.6.3.1.1.1 All Data Registries shall utilize the same informational content, graphical layout and formatting unique to the applicable type of compliance document when displaying the completed compliance documents for review and signing as part of the registration process. These document layouts shall conform to the informational content, graphical layout and formatting approved by the Commission. Additional detailed guidance regarding informational content, graphical layout and formatting will be presented in the Data Registry Requirements Manual.*

##### **JA7.6.3.1.2 Software interfaces**

*JA7.6.3.1.2.1 All registered compliance documents transmitted from any Data Registry shall be secured with the Registration Provider digital signature.*

JA7.6.3.1.2.1.1 All Data Registries shall use the same hash algorithm to generate the document's message digest for the digital signature.

JA7.6.3.1.2.1.2 All Data Registries shall use the same asymmetrical key encryption for generating the digital signature private and public keys used to encrypt and decrypt the message digest.

JA7.6.3.1.2.1.3 Registration Providers shall provide their digital certificate which contains their digital signature public key to any other software entity that receives registered compliance documents from their Data Registry, in particular the Commission document repository.

JA7.6.3.1.2.1.4 The Commission document repository, which will receive registered compliance documents electronically from Data Registries, will have to implement digital signature processing capability in order to perform automatic verification and validation processing on received documents.

JA7.6.3.1.2.1.5 Users who take advantage of digital signature automated verification capabilities to verify the authenticity of registered compliance documents received from Data Registries will have to implement digital signature processing capability in order to perform automatic verification and validation processing on received documents. The Adobe Reader software tool, which is freeware, has the capability to process the digital signatures for any digitally signed documents that utilize standardized digital signature technology.



*JA7.6.3.1.2.2 All Data Registries shall implement the same security protocol for importing completed compliance document transmittals generated by 3rd party software tools. The security protocol shall be approved by the Commission.*

JA7.6.3.1.2.2.1 Guidance shall be provided in the 2016 ACM Reference Manual and the 2016 Data Registry Requirements Manual to assist all 3rd party software entities in implementing the required security protocols.

### **JA7.6.3.2 Functions**

#### **JA7.6.3.2.1 Electronic Signature Capability**

The Data Registry shall provide electronic signature capability to authorized users who have the role of Documentation Author, Field Technician, or Registration Signer. A Field Technician Signature is required only on Certificate of Acceptance Documentation. A Certificate of Acceptance document requires that there be both a Documentation Author signature and a Field Technician signature prior to registration signing.

*JA7.6.3.2.1.1 Any authorized user of a Data Registry can request an electronic signature in order to sign compliance documents as the documentation author, Field Technician, or as the registration signer.*

*JA7.6.3.2.1.2 Registration Providers shall gather and verify any and all information necessary to validate a user applicant's identity and applicable qualifications as prerequisite to authorizing assignment to a user applicant an electronic signature, or permissions as a documentation author, Field Technician, or Registration Signer.*

*JA7.6.3.2.1.3 Authorized users shall provide to the Data Registry an electronic image of their handwritten signature for use in displaying their electronic signature.*

#### **JA7.6.3.2.2 Document Data Validation**

The Data Registry shall check that compliance documents are complete and shall perform the required data validation for the document before making them available for signing and/or registering. The guidance for the data validation for each document shall be provided in the Data Registry Requirements Manual.

Any applicable error messages shall be posted indicating the actions necessary as prerequisite to completion of the registration process.

*JA7.6.3.2.2.1 When a documentation author indicates that the compliance document is complete and he/she is ready to sign it, the Data Registry shall verify that all information necessary to complete the document has been provided as prerequisite to making the signing functionality available to the documentation author.*

*JA7.6.3.2.2.2 The Data Registry shall verify that a compliance document is complete and has received the documentation author's signature as prerequisite to making the compliance document available for registration signing. For Certificate of Acceptance documents, both the Documentation Author and the Field Technician signatures shall be provided as prerequisite to making the document available for registration signing.*

#### **JA7.6.3.2.3 Signer Review and Signature Actions**

The Data Registry shall provide functionality for authorized users to select, review and sign compliance documents as a documentation author, field technician, or registration signer.

*JA7.6.3.2.3.1 The documentation author can electronically sign a compliance document if it has been verified as complete by the Data Registry.*

*JA7.6.3.2.3.2 The Field Technician can electronically sign a Certificate of Acceptance document if it has been verified as complete by the Data Registry and has the documentation author's signature.*

*JA7.6.3.2.3.3 The registration signer can electronically sign a compliance document if it has been verified as complete by the Data Registry and has the documentation author's signature. For Certificate of Acceptance documents both the Documentation Author signature and the Field Technician signature are prerequisite to allowing registration signing.*

*JA7.6.3.2.3.4 When an authorized user selects to sign a compliance document, the Data Registry provides a display of the compliance document layout that allows the user access to any part of the compliance document for review, as well as a display of the declaration statement.*

JA7.6.3.2.3.4.1 All compliance documents shall include a declaration statement applicable to the documentation author signature. The declaration statement language shall be approved by the Commission.

JA7.6.3.2.3.4.2 All Certificate of Acceptance documents shall include a declaration statement applicable to the field technician signature. The declaration statement language shall be approved by the Commission.

JA7.6.3.2.3.4.3 All compliance documents shall include a declaration statement applicable to the registration signer signature. The declaration statement language shall be approved by the Commission.

JA7.6.3.2.3.4.4 All compliance document layouts displayed shall conform to the same format, informational order, and content approved by the Commission. Guidance for data and layout specifications shall be published in the Data Registry requirements manual.

*JA7.6.3.2.3.5 When the documentation author activates the signing control to sign the compliance document, the Data Registry shall display the completed documentation author signature block including the documentation author's electronic signature utilizing the visible image of his or her hand written signature, applicable professional qualifications, licenses and/or certificates the documentation author holds, and the date and time the document was signed.*

*JA7.6.3.2.3.6 When the Field Technician activates the signing control to sign the Certificate of Acceptance document, the Data Registry shall display the completed field technician's signature block including the Field Technician's electronic signature utilizing the visible image of his or her hand written signature, applicable professional qualifications, licenses and/or certificates the Field Technician holds, and the date and time the document was signed.*

*JA7.6.3.2.3.7 When the registration signer activates the signing control to register the compliance document, the Data Registry shall display the completed signature block including the registration signer's electronic signature utilizing the visible image of his or her hand written signature, applicable professional qualifications, licenses or certificates the registration signer holds, the date and time the document was signed, with the newly generated registration number appended to the footer of each of the pages of the document. The registration numbering convention shall conform to the requirements given Reference Joint Appendix JA7.5.4.*

#### **JA7.6.3.2.4 Digital Signatures**

The Data Registry shall apply the Registration Provider digital signature to compliance documents electronically signed by the registration signer and then append the Registration Provider's digital certificate containing their public key, when concluding the document registration procedure in the Data Registry.

*JA7.6.3.2.4.1 When a compliance document is electronically signed by the registration signer, the Data Registry shall apply a visible indication of the Registration Provider's digital signature to the document which shall include the following statement: "This digital signature is provided in order to secure the content of this registered document, and in no way implies Registration Provider responsibility for the accuracy of the information".*

JA7.6.3.2.4.1.1 The Data Registry digital signature software generates a hash number from the contents of the registered compliance document to create the message digest part of the digital signature.

JA7.6.3.2.4.1.2 The Data Registry digital signature software encrypts the message digest using the Registration Provider's digital signature private key to produce the digital signature.

JA7.6.3.2.4.1.3 The Data Registry digital signature software attaches the Registration Provider's digital certificate which contains their digital signature public key to the compliance document, displays the Registration Provider name and logo on each page of the document, and the digital signature's date and time stamp in the footer of each page of the compliance document.

#### **JA7.6.3.2.5 Transmittal to Commission Compliance Document Repository**

The Data Registry, upon completion of the registration procedure, shall immediately and automatically transmit a copy of the completed registered compliance document to the Commission Compliance Document Repository which will process the Registration Provider's digital signature using the Registration Provider's digital certificate to verify the sender and the compliance document contents.

*JA7.6.3.2.5.1 The Data Registry shall transmit the digitally signed and registered compliance document to the Commission document repository using a secure transmission protocol. Detailed guidance for the secure transmission protocol may be specified in the Data Registry Requirements Manual.*

#### **JA7.6.3.2.6 Document Retention**

The Registration Provider shall retain a copy of the completed registered compliance document and make the document available for use by authorized users of the registry who may print a hard copy, or access an electronic copy of the registered document and may subsequently process the Registration Provider's digital signature using their digital certificate to verify the sender and the compliance document contents.

*JA7.6.3.2.6.1 The Data Registry shall provide users the functionality to either view registered documents in their web browser or save the document file to their desktop.*

*JA7.6.3.2.6.2 The Data Registry shall provide functionality to transmit registered compliance documents to authorized requesters.*

*JA7.6.3.2.6.3 The Data Registry shall make their digital signature public key available for all types of authorized access to these registered documents.*

#### **JA7.6.3.2.7 Receive and Process Output From Compliance Software or Other Software Tools**

The Data Registry shall process the Compliance Registration Package transmitted from compliance software tools or other software tools approved by the Commission for use in compliance document registration processes.

*JA7.6.3.2.7.1 The Data Registry shall have functionality to receive data containing electronic documents and data exported from compliance software tools or other software tools approved by the Commission. When data is received using a password protected encrypted file, the file password shall be made available to the Data Registry by the software vendor in a separate secure communication. Additional guidance may be provided in the Data Registry Requirements Manual. The passwords for encrypted data files shall not be made available to the software users or the Data Registry authorized users, or others who do not have the authority to administer the security measures for the compliance software or the registries.*

There may be alternate means by which Compliance Software tools or other software tools approved by the Commission could communicate with Data Registries such as by a Web Service application that may not use encrypted data files, but rather data streaming. Use of such alternate means shall not be allowed unless approved by the Commission.

*JA7.6.3.2.7.2 The Data Registry shall have functionality to decrypt data files it receives that contain completed compliance documents exported from compliance software tools or other software tools approved by the Commission using the password provided by the software vendor. If the password successfully decrypts the file, the Data Registry shall add the compliance document to the registry. Additional guidance describing methods for decrypting data files will be given in the Data Registry Requirements Manual. If the password fails to decrypt the transmitted file, the Data Registry shall display an error message to that effect, and flag any other applicable corrective actions as may be described in the Data Registry Requirements Manual.*

*JA7.6.3.2.7.3 The Data Registry shall only allow the transmission of data between compliance software tools or other software tools approved by the Commission using secure data transfer protocols. Detailed guidance for secure data transfer protocols may be given in the Data Registry Requirements Manual.*

### **JA7.7 Data Exchange Requirements**

Compliance documents are based on standardized data structures that define the content and layout contained for the standard reports that are required by the Administrative Regulations (Title 24, Part 1, §10-103). These data structures will be represented using XML, a well established public data exchange standard developed by the World Wide Web Consortium. All software that generates data used for producing compliance documents, including Data Registries that provide software interfaces for both keyed data entry or data transmission from external systems, will be required to use this technology. Specifically, the data that represents the content in compliance documents will be expressed as XML data which is validated against an XML schema that shall be approved by the Energy Commission. The XML schema will standardize the organization of the data and the terminology and data types, which will strengthen data integrity and provide built-in data validation. As an industry standard for data exchange, using XML technology will take advantage of support from numerous XML read and write software tools that are available in all major development environments.

The compliance document images rendered from the data in the XML document shall be consistent with the informational content and graphical layout formatting for the compliance documents approved by the Commission.

Detailed Guidance for use of the data definitions defined in the XML schema, and data formats used to render each of the registered compliance documents utilized for data exchange procedures for the compliance documents shall be provided in the Data Registry Requirements Manual. Consideration shall be given to use of two complimentary XML technologies, Extensible Stylesheet Language Transformation (XSLT) and Extensible Stylesheet Language Formatting Objects (XSL-FO) which would work directly with the data in the Compliance Data Exchange File to transform the data into the required graphical layout for the compliance document.

Data registries shall provide web-based services to authorized users to enable data exchange between the Data Registry and the authorized user's computer system(s).

Data exchange transactions used for Data Registry document registration processes shall be transactions that utilize technology or software that has been approved by the Commission in accordance with Section JA7.8 or JA7.9 as applicable. Use of technology or software that has not been approved by the Commission shall not be allowed.

#### JA7.7.1 Data Exchange Requirements for Document Registration

##### **JA7.7.1.1 Keyed-in Data Entry**

Data Registries shall have the capability to receive data input transmitted from an authorized user's computer system keyboard entry devices and pointing devices when the authorized user has logged on to the Data Registry web service.

##### **JA7.7.1.2 Imports from Software Tools External to a Data Registry**

For document registration procedures that require electronic data or image files be transmitted to a Data Registry, the electronic data or image file transmittals shall conform to the data exchange requirements specified by Section JA7.7.

Any software tool that utilizes data transmission to a Data Registry for purposes of document registration in a Data Registry shall be a Compliance Software tool approved by the Commission pursuant to all applicable requirements in Title 24 Part 1, Section 10-109, or shall be approved for use in accordance with all applicable requirements in Section JA7.9.

**JA7.7.1.3 Image File Format for Document Registration**

Image files transmitted to a Data Registry from a compliance report generator as part of document registration procedures shall be non-editable "flat" image files in pdf format. Registered document images produced by a Data Registry shall be non-editable "flat" image files in pdf format. The pdf image shall not be recreated from data every time a user wishes to view the registered document. The image shall be generated only once, and stored as a "non-editable" image file.

**JA7.7.1.4 Export to Commission Compliance Document Repository**

Contingent upon approval of a document repository by the Commission, upon conclusion of the registration of a document, the Data Registry shall immediately and automatically export a copy of the registered compliance document to the Commission Document Repository. The export shall conform to the specifications for data exchange described in JA7.7 and consist of an XML file which is validated against an XML schema. The xml schema shall be approved by the Energy Commission. Detailed guidance for data and document exports to the document repository may be included in the Data Registry Requirements Manual.

Exports to the Commission Compliance Document Repository shall contain the data represented on the registered compliance document, and the Registration Provider's digitally signed image file that represents the completed registered compliance document.

**JA7.7.1.5 Electronic Copies of Registered Compliance Documents for Submittals**

Registered document files retained by a Data Registry shall be made available to authorized users of the Data Registry for download for use for electronic submittals. These electronic copies of the registered compliance documents shall have the Registration Provider's digital signature which provides for automatic electronic verification of the authenticity of the document. Refer to Section JA7.5.5 for more information about automatic verification of document authenticity using digital certificates.

## **JA7.8 Data Registry Approval**

This section explains the requirements for approval of Data Registries that provide services to authorized users for creating and registering documents required for compliance with Part 6.

The Commission shall perform acceptance testing of Data Registries when a Registration Provider applicant submits an application in order to determine if the requirements in Reference Joint Appendix JA7 have been met.

Detailed guidance for approval of data registries may be provided in the Data Registry Requirements Manual.

### JA7.8.1 Overview

The approval procedure requires self-testing and self-certification by the Registration Provider applicant. The Registration Provider applicant shall conduct the specified tests, evaluate the results and certify in writing that the Data Registry passes the tests. The Commission shall perform spot checks and may require additional tests to verify that the proposed Data Registry is suitable for use for providing the compliance document registration functionality required by the Standards. The Registration Provider shall develop a user manual or online help screens that explain how to perform the document registration procedures offered by the Data Registry. The user manual or online help screens shall be reviewed by the Commission for accuracy and ease of use.

### JA7.8.2 Application Checklist

Application for approval shall conform to all applicable requirements given in Standards Section 10-109. The following is a list of the items that shall be included in an application package:

#### **JA7.8.2.1 Registration Provider Applicant Certification Statement.**

A statement from the Registration Provider applicant certifying the reliability and accuracy of the Data Registry when used for registration of Compliance Documents in accordance with the requirements of Standards Section 10-103(a), Reference Joint Appendix JA7, and may reference the guidance given in the Data Registry Requirements Manual.

The template for the Registration Provider Certification Statement document may be published in the Data Registry Requirements Manual, and electronic versions of the Registration Provider Certification Statement template shall be made available to Registration Provider applicant upon request.

#### **JA7.8.2.2 Compliance Document Registration Test Results.**

Electronic copies of the results of the data exchange verification tests, and electronic copies of the registered documents that result from the document registration tests shall be provided. Detailed guidance to assist the applicant in performing and reporting the standardized tests may be given in the Data Registry Requirements Manual.

#### **JA7.8.2.3 User Manual**

A copy of the user manual for the Data Registry shall be provided in an electronic format that can be utilized by word processing software. Help screens from the Data Registry user interface, organized into an electronic document file with a table of contents is an acceptable alternative to the requirement for a user manual.

#### **JA7.8.2.4 Data Registry Authorized User Account Access.**

User name and password information shall be provided to allow access to the Data Registry for Commission staff to perform verification of Data Registry functionality.

The Registration Provider's digital signature public key shall be provided in order that their digital signature on registered documents can be tested.

### **JA7.8.2.5 Application Fee and Other Administrative Requirements**

Refer to Standards Section 10-109 for required application fees and additional administrative requirements applicable to approval of data registries.

#### JA7.8.3 Types of Approval

There are two Data Registry approval procedures: full approval, and amendment to full approval. Full approval is required for all Data Registry changes unless they qualify for the amendment to full approval procedure.

### **JA7.8.3.1 Full Approval**

Full approval is required when an applicant Data Registry service has not previously been approved by the Commission. Additionally, the Commission may require that all Data Registries conform to the requirements of a full approval procedure when the Standards are updated (re-approval), or whenever substantial changes are made to a Data Registry's functionality, security, or technology features. When Data Registry re-approval is mandated by the Commission, all Registration Providers shall be notified of the re-approval timetable. A revised Data Registry Requirements Manual may be published to provide guidance for the re-approval process.

Full approval shall ensure the Data Registry conforms to all applicable requirements for functionality and security in JA7 including but not limited to:

- (a) Capability to produce and manage registered documents (JA7.5).
- (b) Electronic signature capability, and manage authorization of users (JA7.6.3.2.1).
- (c) Document data validation (JA7.6.3.2.2).
- (d) Signer review and signature actions (JA7.6.3.2.3).
- (e) Digital signature and digital certificate actions (JA7.6.3.2.4).
- (f) Capability to transmit secured documents and data to the Commission Compliance Document Repository (JA7.6.3.2.5).
- (g) Document retention capability (JA7.6.3.2.6).
- (h) Capability to receive and process secured output files from compliance software and other software tools approved for use for registering compliance documents (JA7.6.3.2.7).
- (i) Capability for data exchange with compliance report generation services approved by the Commission to generate formatted electronic documents (JA7.7).

Detailed guidance to assist with approval procedures may be given in the Data Registry Requirements Manual.

### **JA7.8.3.2 Amendments**

Certain types of changes to Data Registry software applications may be made through a streamlined amendment process. Changes that qualify for amendment approval are changes for which there are minor changes to the document registration procedures, data input requirements, or registered documentation output for the Data Registry. When Data Registry modifications qualify for amendment approval, the following procedure shall be followed:

- (a) The Registration Provider applicant shall notify the Commission in writing to provide a description of the change and the reason for making the change.



- (b) The Registration Provider applicant shall prepare an addendum to the user manual describing the change to the Data Registry if applicable.
- (c) The Commission shall respond to the Registration Provider applicant within 45 days. The Commission response to the applicant may:
1. approve the modification;
  2. request additional information;
  3. refuse to approve the modification;
  4. require the Registration Provider to submit results of additional acceptance tests applicable to the modification; or
  5. require that the Registration Provider make specific changes to either the User Manual addendum or the Data Registry functionality.

The Registration Provider shall submit results of any required validation tests applicable to the modification. It is not necessary to resubmit Data Registry test results previously submitted that remain valid.

Any amendment to an existing Data Registry approval shall be accompanied by a cover letter explaining the type of amendment requested, and copies of any other applicable documents that are required. All items on the application checklist shall be submitted, when applicable. The timetable for approval of amendments is the same as for full approval.

- (d) With Commission approval, the Registration Provider may make the modified Data Registry available for use for registration of compliance documentation, along with the modified user manual or addendum to the user manual, and shall notify authorized users of the Data Registry.

#### JA7.8.4 Rescinding Approval (Deactivation) of Data Registries

The Commission may rescind approval of Data Registries through various means.

##### **JA7.8.4.1 Procedures that Initiate Deactivation**

- (a) All Data Registries are deactivated when the Standards undergo substantial changes, usually occurring with each Standards update. However, the Data Registry shall remain approved to provide document registration for projects that have been permitted under the prior versions of the Standards.
- (b) Any Data Registry can be deactivated by a letter from the Registration Provider requesting that the Data Registry be deactivated. The deactivation request shall briefly describe the reasons that justify the need for deactivation.
- (c) Any "initiating party" may commence a procedure to deactivate a Data Registry according to the steps outlined below. The intent is to provide a means whereby serious Data Registry errors, flawed numeric results, improper registered document output not discovered in the Data Registry approval process can be verified, and a corrective course of action determined. In this process, there is ample opportunity for the Commission, the Registration Provider, and all interested parties to evaluate any alleged errors in the Data Registry functionality.

##### **JA7.8.4.2 Challenging a Data Registry and Initiating Deactivation**

A description of the process for challenging a Data Registry or initiating a deactivation procedure follows:

- (a) Any party may initiate a review of a Data Registry approval by sending a written communication to the Commission's Executive Director. (The Commission may be the initiating party for this type of review by noticing the availability of the same information listed here.) The initiating party shall:
1. State the name of the Data Registry that contains the alleged errors;

2. Identify concisely the nature of the alleged errors in the Data Registry that require review;
  3. Explain why the alleged errors are serious enough in their effect on document registration compliance to justify a deactivation procedure; and
  4. Include appropriate data electronically (in a format agreed to by the Commission staff) and/or information sufficient to evaluate the alleged errors.
- (b) The Executive Director shall make a copy or copies of the initial written communication available to the Registration Provider and interested parties within 30 days. Comments from interested parties shall be received within 60 days of the acceptance of the original application.
  - (c) Within 75 days of receipt of the written communication, the Executive Director may request any additional information needed to evaluate the alleged Data Registry errors from the party who initiated the deactivation review process. If the additional information is incomplete, this procedure will be delayed until the initiating party submits complete information.
  - (d) Within 75 days of receipt of the initial written communication, the Executive Director may convene a workshop to gather additional information from the initiating party, the Registration Provider and interested parties. All parties will have 15 days after the workshop to submit additional information regarding the alleged program errors.
  - (e) Within 90 days after the Executive Director receives the application or within 30 days after receipt of complete additional information requested of the initiating party, whichever is later, the Executive Director shall either:
    1. Determine that the Data Registry need not be deactivated; or
    2. Submit to the Commission a written recommendation that the Data Registry be deactivated.
  - (f) If the Commission approves the Data Registry deactivation, it shall take effect 60 days later. During the first 30 days of the 60 day period, the Executive Director shall send out a Notice to Enforcement Agencies and Interested Parties announcing the deactivation.

#### **JA7.8.4.3 Burden of Proof**

All initiating parties have the burden of proof to establish that the review of alleged Data Registry errors should be granted. The deactivation process may be terminated at any time by mutual written consent of the initiating party and the Executive Director.

The Registration Provider may use the 180 to 210-day period outlined here to update the Data Registry, get it re-approved by the Commission, and make available for use by authorized users, the revised version of the Data Registry that does not contain the errors initially brought to the attention of the Commission.

#### JA7.8.5 Data Registry User Manual

Each Registration Provider is required to publish a Data Registry User Manual. This requirement may be met ~~with-by incorporating~~ help screens ~~incorporated~~ into the Data Registry user interface, however, a printed version which includes all help screen items must be submitted with the application. The Data Registry User Manual ~~provides-shall provide~~ guidance for building permit applicants and enforcement agency officials to enable correct use of the Data Registry, and assists with preparation of registered documentation used for submittals to enforcement agencies and other parties to the construction project.

The Document Registration Manual shall describe the specific Data Registry procedures for completing registered compliance documents. The manual shall provide instructions for preparing the data input and utilizing the registered documents for submittals. An example of a full set of compliance documents for a building project shall be included.

Data Registry User Manuals shall be written in a clear and concise manner and with an organization and format that will allow users to quickly locate the topic and understand the instructions. Also, Registration

Providers shall make electronic copies of their user manual available from their Data Registry website to all building departments in California.

The following sections describe the information that shall be included in all Data Registry User Manuals. It also presents the required organization for that information.

#### **JA7.8.5.1 Energy Commission Approval**

This section includes a copy of the official Energy Commission notice of approval of the Data Registry. It shall include the date of approval, and may include an expiration date for approval as well. The Energy Commission will provide this notice upon completion of evaluation and approval of the Data Registry service.

#### **JA7.8.5.2 Data Registry Capabilities**

This section shall discuss the Data Registry capabilities, providing explanation of how to access these capabilities, and the purpose for each of these features. Reference may be made to sections of the Data Registry Users Manual for more complete description.

#### **JA7.8.5.3 Preparing Basic Documents**

This section shall cover the basic use of the Data Registries to prepare each of the basic Compliance Document types. Reference may be made to the users' manual, but this section should include a complete summary of all document creation methods or commands necessary to complete the required registered documents.

#### **JA7.8.5.4 Instruction for Submittal of the Registered Document(s)**

This section shall contain instruction for completing submittals of completed registered documents to enforcement agencies or other persons who require copies of completed registered documents. Instruction shall be given for all methods of submittal the Data Registry supports, including various methods for submittal of electronic copies of the registered documents, as well as for printing of paper copies

#### **JA7.8.5.5 Sample Compliance Documentation**

This section shall include an example of a complete set of compliance documentation for a sample building. The building need not be overly complex, nor need it include every document type possible. The example should, however, include example documentation for all Compliance document types that would normally be submitted for any occupancy types administered by the Data Registry.

---

### **JA7.9 Approval of Software-Digital Data Sources Used for Data Input to Data Registries**

This section explains the requirements for approval of software-digital data sources used for data input to data registries for creating and registering documents required for compliance with Part 6.

The Commission shall perform acceptance testing of software-the data transfer procedures used for document registration procedures when a software data source vendor -and a Data Registration Provider applicant submits an application in order to determine if the applicable requirements in Reference Joint Appendix JA7 have been met.

Detailed guidance for approval of software may be provided in the Data Registry Requirements Manual.

Note: JA7.9 does not apply to approval of compliance software used for the performance method for demonstrating compliance with Part 6.

### JA7.9.1 Overview

The approval procedure requires self-testing and self-certification by the software vendor applicant. The software vendor applicant shall conduct the specified tests, evaluate the results and certify in writing that the software passes the tests. The Commission shall perform spot checks and may require additional tests to verify that the proposed software is suitable for use for providing the data input for completion of the compliance documents as required by the Standards. The software vendor shall develop a user manual or online help screens that explain how to perform the data input procedures offered by the software. The user manual or online help screens shall be reviewed by the Commission for accuracy and ease of use.

### JA7.9.2 Application Checklist

Application for approval shall conform to all applicable requirements given in Standards Section 10-109. The following is a list of the items that shall be included in an application package:

#### **JA7.9.2.1 Software Vendor Applicant Certification Statement.**

A statement from the software vendor applicant certifying the reliability and accuracy of the software when used for data input to Data Registries for creating and registering compliance documents in accordance with the requirements of Reference Joint Appendix JA7, and may reference the guidance given in the Data Registry Requirements Manual.

The template for the Software Vendor Certification Statement document may be published in the Data Registry Requirements Manual, and electronic versions of the Software Vendor Certification Statement template shall be made available to Software Vendor applicant upon request.

#### **JA7.9.2.2 Compliance Document Registration Test Results.**

Electronic copies of the results of the data exchange verification tests, and electronic copies of the registered documents that result from the compliance report generator tests shall be provided.

Detailed guidance to assist the applicant in performing and reporting the standardized tests may be given in the Data Registry Requirements Manual.

#### **JA7.9.2.3 User Manual**

A copy of the user manual for the software shall be provided in an electronic format that can be utilized by word processing software. Help screens from the software user interface, organized into an electronic document file with a table of contents is an acceptable alternative to the requirement for a user manual.

#### **JA7.9.2.4 Application Fee and Other Administrative Requirements**

Refer to Standards Section 10-109 for required application fees and additional administrative requirements applicable to approval of software used with data registries.

### JA7.9.3 Types of Approval

There are two software approval procedures: full approval, and amendment to full approval. Full approval is required for all software changes unless they qualify for the amendment to full approval procedure.

#### **JA7.9.3.1 Full Approval**

Full approval is required when an applicant software service has not previously been approved by the Commission. Additionally, the Commission may require that all approved data input software tools conform to the requirements of a full approval procedure when the Standards are updated (re-approval), or whenever substantial changes are made to a software's functionality, security, or technology features. When software re-approval is mandated by the Commission, all software vendors shall be notified of the re-

approval timetable. A revised Data Registry Requirements Manual may be published to provide guidance for the re-approval process.

Full approval shall ensure the software conforms to all applicable requirements for functionality and security in JA7 including but not limited to:

- (a) Document data validation (JA7.6.3.2.2)
- (b) Capability for data exchange with compliance report generation services approved by the Commission to generate formatted electronic documents (JA7.7),

Detailed guidance to assist with approval procedures may be given in the Data Registry Requirements Manual.

### **JA7.9.3.2 Amendments**

Certain types of changes to software applications may be made through a streamlined amendment process. Changes that qualify for amendment approval are changes for which there are minor changes to the document registration procedures, data input requirements, or documentation output for the software. When software modifications qualify for amendment approval, the following procedure shall be followed:

- (a) The software vendor applicant shall notify the Commission in writing to provide a description of the change and the reason for making the change.
- (b) The software vendor applicant shall prepare an addendum to the user manual describing the change to the software if applicable.
- (c) The Commission shall respond to the software vendor applicant within 45 days. The Commission response to the applicant may:
  - 1. approve the modification;
  - 2. request additional information;
  - 3. refuse to approve the modification;
  - 4. require the software vendor to submit results of additional acceptance tests applicable to the modification; or
  - 5. require that the software vendor make specific changes to either the User Manual addendum or the software functionality.

The software vendor shall submit results of any required validation tests applicable to the modification. It is not necessary to resubmit software test results previously submitted that remain valid.

Any amendment to an existing software approval shall be accompanied by a cover letter explaining the type of amendment requested, and copies of any other applicable documents that are required. All items on the application checklist shall be submitted, when applicable. The timetable for approval of amendments is the same as for full approval.

- (d) With Commission approval, the software vendor may make the modified software available for use for registration of compliance documentation, along with the modified user manual or addendum to the user manual, and shall notify authorized users of the software.

### JA7.9.4 Rescinding Approval (Deactivation) of Software

The Commission may rescind approval of software through various means.

#### **JA7.9.4.1 Procedures that Initiate Deactivation**

- (a) All software is deactivated when the Standards undergo substantial changes, usually occurring with each Standards update. However, the software shall remain approved to provide data input to Data Registries for creating and registering compliance documents for projects that have been permitted under the prior versions of the Standards.

- (b) Any software can be deactivated by a letter from the software vendor requesting that the software be deactivated. The deactivation request shall briefly describe the reasons that justify the need for deactivation.
- (c) Any "initiating party" may commence a procedure to deactivate a software tool according to the steps outlined below. The intent is to provide a means whereby serious software errors, flawed numeric results, improper document output not discovered in the software approval process can be verified, and a corrective course of action determined. In this process, there is ample opportunity for the Commission, the software vendor, and all interested parties to evaluate any alleged errors in the software functionality.

#### **JA7.9.4.2 Challenging a Software Tool and Initiating Deactivation**

A description of the process for challenging a software tool or initiating a deactivation procedure follows:

- (a) Any party may initiate a review of a software tool approval by sending a written communication to the Commission's Executive Director. (The Commission may be the initiating party for this type of review by noticing the availability of the same information listed here.) The initiating party shall:
  - 1. State the name of the software that contains the alleged errors;
  - 2. Identify concisely the nature of the alleged errors in the software that require review;
  - 3. Explain why the alleged errors are serious enough in their effect on document registration compliance to justify a deactivation procedure; and
  - 4. Include appropriate data electronically (in a format agreed to by the Commission staff) and/or information sufficient to evaluate the alleged errors.
- (b) The Executive Director shall make a copy or copies of the initial written communication available to the software vendor and interested parties within 30 days. Comments from interested parties shall be received within 60 days of the acceptance of the original application.
- (c) Within 75 days of receipt of the written communication, the Executive Director may request any additional information needed to evaluate the alleged software errors from the party who initiated the deactivation review process. If the additional information is incomplete, this procedure will be delayed until the initiating party submits complete information.
- (d) Within 75 days of receipt of the initial written communication, the Executive Director may convene a workshop to gather additional information from the initiating party, the software vendor and interested parties. All parties will have 15 days after the workshop to submit additional information regarding the alleged program errors.
- (e) Within 90 days after the Executive Director receives the application or within 30 days after receipt of complete additional information requested of the initiating party, whichever is later, the Executive Director shall either:
  - 1. Determine that the software need not be deactivated; or
  - 2. Submit to the Commission a written recommendation that the software be deactivated.
- (f) If the Commission approves the software deactivation, it shall take effect 60 days later. During the first 30 days of the 60 day period, the Executive Director shall send out a Notice to Data Registries, Enforcement Agencies, and other Interested Parties announcing the deactivation.

#### **JA7.9.4.3 Burden of Proof**

All initiating parties have the burden of proof to establish that the review of alleged software errors should be granted. The deactivation process may be terminated at any time by mutual written consent of the initiating party and the Executive Director.

The software vendor may use the 180 to 210-day period outlined here to update the software, get it re-approved by the Commission, and make available for use by authorized users, the revised version of the software that does not contain the errors initially brought to the attention of the Commission.

#### JA7.9.5 Software User Manual

Each software vendor is required to publish a Software User Manual. This requirement may be met with help screens incorporated into the software user interface, however, a printed version which includes all help screen items must be submitted with the application. The Software User Manual provides guidance for building permit applicants and enforcement agency officials to enable correct use of the software, and assists with preparation of registered documentation used for submittals to enforcement agencies and other parties to the construction project.

The Software User Manual shall describe the specific software procedures for completing compliance documents for use for registration. The manual shall provide instructions for preparing the data input and utilizing the completed formatted documents for registration.

Software User Manuals shall be written in a clear and concise manner and with an organization and format that will allow users to quickly locate the topic and understand the instructions. Also, software vendor shall make electronic copies of their user manual available from their Software product website to all building departments in California.

The following sections describe the information that shall be included in all software user manuals. It also presents the required organization for that information.

##### **JA7.9.5.1 Energy Commission Approval**

This section includes a copy of the official Energy Commission notice of approval of the software tool. It shall include the date of approval, and may include an expiration date for approval as well. The Energy Commission will provide this notice upon completion of evaluation and approval of the software tool.

##### **JA7.9.5.2 Software Capabilities**

This section shall discuss the software capabilities, providing explanation of how to access these capabilities, and the purpose for each of these features.

##### **JA7.9.5.3 Preparing Basic Documents**

This section shall cover the basic use of the software to prepare each of the applicable Compliance Document types. Reference may be made to the users' manual, but this section should include a complete summary of all document creation methods or commands necessary to complete the required compliance documents.

##### **JA7.9.5.4 Sample Compliance Documentation**

This section shall include an example of the applicable compliance documentation for a sample building. The building need not be overly complex, but the example should, however, include example documentation for all Compliance document types that would normally be submitted for any occupancy types administered by the Data Registry.

---

#### **JA7.10 Related Publications**

The Compliance Supplement should refer users to the following related Energy Commission publications and where to obtain them:

- (a) 2016 Building Energy Efficiency Standards (publication number unknown at time of printing)

- (b) 2016 Joint Appendices (publication number unknown at time of printing)
- (c) 2016 ACM Approval Manual (publication number unknown at time of printing)
- (d) 2016 Residential Compliance Manual (publication number unknown at time of printing)
- (e) 2016 Nonresidential Compliance Manual (publication number unknown at time of printing)
- (f) 2016 Data Registry Requirements Manual (publication number unknown at time of printing)
- (g) 2016 ACM Reference Manual (publication number unknown at time of printing)

These publications are available from:

California Energy Commission  
Publications Unit  
1516 Ninth Street  
Sacramento CA 95814  
(916) 654-5200