

VOLUME 3 GENERAL TECHNICAL ADMINISTRATION**CHAPTER 31 ELECTRONIC SIGNATURES, ELECTRONIC RECORDKEEPING SYSTEMS, AND ELECTRONIC MANUAL SYSTEMS****Section 2 Requirements for Approval, Acceptance, and Authorization**

3-2999 BACKGROUND. The Government Paperwork Elimination Act (GPEA) (Public Law (PL) 105-277, Title XVII); the Electronic Signatures in Global and National Commerce Act (E-Sign) (PL 106-229); and the Office of Management and Budget (OMB) Memorandum 00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, encourage the use of electronic records, signatures, and alternative information technologies, and allow Government agencies to develop performance standards for their use. The use of these electronic technologies also supports the goals of the Small Business Paperwork Relief Act of 2002 (SBPRA) (H.R. 327). This section sets forth the Federal Aviation Administration (FAA) performance standards for a certificate holder's use of electronic manual systems, electronic recordkeeping systems, and electronic signatures.

3-3000 GENERAL. This section contains information on the overall standards for approval or acceptance, and authorization of an electronic signature process, electronic recordkeeping system, or electronic manual system. This information applies to aviation safety inspectors (ASI) and principal inspectors (PI) with oversight responsibility of regulated entities (e.g., certificate holders, program managers, operators, air agencies, and Organization Designation Authorization (ODA) holders) that are subject to the Title 14 of the Code of Federal Regulations (14 CFR) requirements for manuals, records, and signatures. For simplicity, this chapter uses the singular term "certificate holder" to describe these entities.

3-3001 SCOPE. The policy and standards for electronic signatures, records, and manuals as described in this section apply where these items are required by 14 CFR. This policy is not intended for application beyond those regulatory requirements. In general, the categories of signatures, records, and manuals this policy applies to are as follows: (This is not intended to be an all-inclusive list of categories.)

A. Signatures:

- Certification of Training or Qualification;
- Pilot Logbooks;
- Fitness for Duty;
- Flight/Dispatch Release;
- Load Manifests;
- Operational Control Briefing;
- Maintenance Logbook;
- Airworthiness Release;
- Maintenance Performed; and
- Continuous Airworthiness Maintenance Program (CAMP) Extended Operations (ETOPS) Pre-departure Service Check.

B. Records:

- Training and Qualification;
- Crewmember;
- Dispatcher;
- Flight, Duty and Rest;
- Dispatch Release;
- Flight Release;
- Load Manifest;
- Communication;
- Maintenance Records;
- Maintenance Log;
- Airworthiness Release;
- ODA Records and Reports; and
- Effective March 9, 2018, Safety Management System (SMS) Records required by 14 CFR Part 5, § 5.97.

C. Manuals:

- Flight Operations (including dispatch, flight following, and onboard/cabin);
- Ground Operations (including ground and passenger handling);
- Certificate Holder Aircraft Performance manuals (Airplane Flight Manual (AFM) and Weight and Balance (W&B) information, etc.);
- Training Program;
- Maintenance (including overhaul, standard practices, etc.);
- Minimum equipment list (MEL);
- General Policy and Procedures; and
- User (e.g., Flight Management System (FMS), Flight Planning System, etc.).

3-3002 REGULATORY REFERENCES AND GUIDANCE MATERIAL. Refer to the current editions of the following:

- Electronic Signatures in Global and National Commerce Act (E-Sign) (PL 106-229, Title I).
- Government Paperwork Elimination Act (GPEA) (PL 105-277, Title XVII).
- Paperwork Reduction Act of 1995 (PL 104-13).
- OMB Memorandum 00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act.
- Digital Signature Guidelines—American Bar Association Legal Infrastructure for Certification Authorities and Secure Electronic Commerce.
- Advisory Circular (AC) 91-78, Use of Class 1 or Class 2 Electronic Flight Bag (EFB).
- AC 91.21-1, Use of Portable Electronic Devices Aboard Aircraft.
- AC 120-64, Operational Use and Modification of Electronic Checklists.

- AC 120-70, Operational Authorization Process for Use of Data Link Communication System.
- AC 120-76, Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags.
- AC 120-78, Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals.

3-3003 RELATED POLICY. Additional policy related to electronic signatures and records is available in the following locations:

A. Volume 3, Chapter 25, Section 1:

1) Title 14 CFR Part 121 Dispatch and Flight Release Requirements – Electronic Signatures, Amendments, and Disposition. Volume 3, Chapter 25, Section 1, contains information regarding electronic signatures on a dispatch or flight release, electronic amendments to a dispatch or flight release, and electronic recordkeeping of a dispatch or flight release.

2) Part 121 En Route Communication Records. Volume 3, Chapter 25, Section 1, also contains information on the electronic retention of en route communication records in accordance with part 121, § 121.711.

B. Volume 3, Chapter 31, Section 3 – Part 121 and 14 CFR Part 135 Crewmember and Aircraft Dispatcher Records. Volume 3, Chapter 31, Section 3, contains detailed information regarding crewmember and aircraft dispatcher records in accordance with the requirements of parts 121 and 135, as applicable.

C. Volume 3, Chapter 31, Section 5 – Part 121 and Part 135, § 135.411(a)(2) Maintenance Records. Volume 3, Chapter 31, Section 5, contains detailed information regarding the evaluation of an air carrier’s maintenance recordkeeping system.

D. Volume 3, Chapter 31, Section 6 – 14 CFR Part 91K Non-CAMP Program Manager’s, 14 CFR Part 125, § 125.247 Certificate Holder’s, and § 135.411(a)(1) Maintenance Records. Volume 3, Chapter 31, Section 6, contains information for Airworthiness inspectors on how to evaluate part 91K non-CAMP and part 135 maintenance records.

E. Volume 3, Chapter 18, Section 3 – Part A Operations Specifications (OpSpecs): OpSpec A025, Authorization to Use an Electronic Signature, Electronic Recordkeeping System, or Electronic Manual System. Volume 3, Chapter 18, Section 3, Part A OpSpecs, OpSpec/Management Specification (MSpec) A025, contains information on how to populate the A025 templates.

F. FAA Order 8000.79, Use of Electronic Technology and Storage of Data (current edition).

3-3004 APPROVAL, ACCEPTANCE, AND AUTHORIZATION REQUIREMENTS FOR 14 CFR PARTS 91K, 121, 125, 133, 135, 141, 142, 145, AND 147. The regulatory parts under 14 CFR contain varying requirements that mandate whether or not an electronic signature, record, or manual requires approval, acceptance or authorization.

A. Approval Required. A certificate holder requires FAA approval to use the following electronic manual and recordkeeping system.

1) **Electronic MEL – Parts 91K, 121, 125, and 135.** In accordance with part 91, § 91.115, § 121.628, § 125.201, and § 135.179, certificate holders conducting part 91K, 121, 125, or 135 operations are required to provide direct MEL access to flightcrew members through printed or other means approved by the Administrator. Therefore, a certificate holder requires FAA approval to provide electronic access to the MEL to its flightcrew members.

2) **Part 121 Crewmember and Dispatcher Records.** Section 121.683 allows a certificate holder conducting part 121 operations to use a computer (electronic) record system that is approved by the Administrator to record and maintain crewmember and dispatcher records.

3) **Part 125 Crewmember Records.** Section 125.401 allows a certificate holder conducting part 125 operations to use a computer record system that is approved by the Administrator to record and maintain crewmember records.

B. Acceptance Required – Parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147. In accordance with the regulatory requirements contained in parts 91K, 121, 125, 133, 135, 141, 142, 145, 147, OpSpec requirements, and FAA policy, a certificate holder requires FAA acceptance to use the following electronic items.

1) **Electronic Manuals.** Electronic entry, maintenance, storage, and distribution of the manuals required by parts 91K, 121, 125, 133, 135, and 145 requires FAA acceptance.

2) **Electronic Records.** Using an electronic system to enter, modify, maintain, store, and/or make available the records required by parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147 requires FAA acceptance.

3) **Electronic Signature Process.** For parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147 operations, an electronic signature process requires FAA acceptance.

C. OpSpec Authorization Required. The term “OpSpec,” when used in this section, means any authorization contained in the Web-based Operations Safety System (WebOPSS).

1) **Parts 91K, 121, 125, 133, 135, and 145.** Certificate holders conducting operations in accordance with parts 91K, 121, 125, 133, 135, and 145 require OpSpec authorization by the FAA to use an electronic signature, electronic recordkeeping system, or electronic manual system.

2) **Parts 141, 142, and 147.** Part 141 pilot schools, part 142 training center operators, and part 147 Aviation Maintenance Technician Schools (AMTS) require OpSpec authorization to use an electronic recordkeeping system and electronic signatures in conjunction with that recordkeeping system.

D. Use OpSpec A025 as the Method to Approve, Accept, and Authorize Use.

The certificate-holding district office (CHDO) will use OpSpec A025 as the method to convey FAA approval or acceptance of a certificate holder's electronic signature process, electronic manual system, or electronic recordkeeping system. The signature on the OpSpec of the PI or ASI with OpSpec signature authority indicates the FAA's approval or acceptance (depending on the requirement). When the PI or ASI issues the OpSpec in WebOPSS, the certificate holder is authorized to use the electronic items listed in A025 as of the effective date of the active OpSpec. This date also signifies the effective date of FAA approval or acceptance. Information on how to issue A025 is contained in Volume 3, Chapter 18, Section 3.

3-3005 THERE IS NO REQUIREMENT FOR FORMAL APPROVAL, ACCEPTANCE, OR AUTHORIZATION FOR 14 CFR PARTS 61, 63, 65, 91 (EXCLUDING 91K), 129, 137, OR 183. The use of an electronic signature, electronic recordkeeping system, or electronic manual system under part 61, 63, 65, 91 (excluding 91K), 129, 137, or 183 does not require formal FAA approval, acceptance, or authorization. OpSpec (including an MSpec/training specification (TSpec)/letter of authorization (LOA)) A025 does not apply to operations under these parts. However, the FAA's standards for electronic signatures, records, and manuals should always apply regardless of whether or not approval, acceptance, or authorization is required. If a required signature, record, or manual is provided in an electronic format or application that does not meet the FAA's standards set forth in this section and AC 120-78, the FAA may question its validity. Should the FAA determine that an electronic signature, recordkeeping system, or manual system does not meet these standards or is otherwise unacceptable, the CHDO will notify the certificate holder in writing. Upon receiving notification, it is incumbent upon the certificate holder to make the appropriate corrections.

NOTE: Part 61, § 61.55, which applies to second-in-command (SIC) qualifications, requires an applicant whose flight experience and/or training records are in an electronic form to present a paper copy of those records containing the signature of the trainer or qualified management official to an FAA Flight Standards District Office (FSDO) or examiner.

3-3006 ELECTRONIC SIGNATURES. According to the U.S. Electronic Signatures in Global and National Commerce Act (PL 106-229 (also known as E-Sign)), an electronic signature is an "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." The process of affixing an electronic signature must include authentication of the signatory's identity; permanently binding the signature to the intended document, record, or data; and non-alterability of the document, record, or data once the signature has been affixed. To be considered valid, an electronic signature must provide equivalent qualities and attributes to those that are identified with a handwritten signature. A handwritten signature is universally accepted because it typically contains qualities and attributes that are unique and can easily be identified as belonging to the individual signatory. The simple appearance of an individual's name depicted

electronically would not typically have the same force and effect as a handwritten signature; nor would it confirm that the individual whose name appears had any intention of affixing his or her signature. Electronic signatures can be broken down into these components:

- A method of signing,
- User authentication,
- Data authentication, and
- Capture of the signatory's intent to sign.

A. Types of Electronic Signatures. Electronic signatures may appear in various formats. In order to be considered valid, each electronic signature must meet the FAA's standards for electronic signatures that appear in subparagraph 3-3006B below. The simple entry or appearance of an individual's name in an electronic format does not constitute an electronic signature. Examples of electronic signature formats include, but are not limited to:

- A digital signature;
- A digitized image of a handwritten signature that is attached to an electronic record;
- An electronic code (e.g., a secret code, password, or PIN) used by a person to sign the electronic record; and
- A unique biometrics-based identifier, such as a fingerprint, voice print, or retinal scan.

B. FAA Standards for Electronic Signatures. All electronic signatures must meet the following standards in order to be considered legally binding.

- 1) The Signatory Must Use an Acceptable Electronic Signature.**
- 2) The Signature Must Be Unique to the Signatory.** An electronic signature is only valid if it is unique to the individual signatory.
- 3) There Must Be a Means to Identify and Authenticate the Signer.** A valid electronic signature must include a means to authenticate a particular person as being the one affixing the signature.
- 4) The Signature Must Be Under the Sole Control of the Signatory.** A valid electronic signature must be under the sole control of the signatory. The system or application used to actually sign a record or document must require the signatory to use a unique user name and password to access the system and affix the signature.
- 5) Intent to Sign.** The electronic signature must be executed or adopted by a person with the intent to sign the electronic record or document. The signature must indicate the signer's approval, affirmation, or verification of the information contained in the electronic record or document.

6) The Signature Must Be Permanent and the Information Must Be Unalterable Without a New Signature. A valid electronic signature must be a permanent part of the record or document to which it was affixed. The information contained in the record or document must be unalterable without a new signature to validate the alteration (any change to the original information as original signed for by the signatory).

7) Preservation of Signed Record or Document. There must be a means to preserve the integrity of the electronically signed record or document.

8) Deliberate Action. An individual using an electronic signature should take deliberate and recognizable action to affix his or her signature. Acceptable, deliberate actions for creating a digital electronic signature include, but are not limited to, the following:

- Using a digital signature,
- Entering a user name and password,
- Swiping a badge, and
- Using an electronic stylus.

9) Non-Repudiation. A valid electronic signature must prevent the signatory from denying that he or she affixed a signature to a specific record, document, or body of data.

10) A Valid Electronic Signature Will Not Be Denied Legal Effect or Enforceability. In accordance with the Electronic Signatures in Global and National Commerce Act (E-Sign) (PL 106-229), electronic documents, records, or data that contain a valid electronic signature or authentication, will not be denied legal effect, validity, or enforceability due to the electronic format.

C. Compliance with Recordkeeping Requirements. An electronic signature that is affixed to any record required by 14 CFR part 91K, 121, 125, 133, 135, 141, 142, 145, or 147 requires a certificate holder to have an FAA-approved or FAA-accepted (depending on the regulatory requirement) electronic recordkeeping system. Electronic recordkeeping system standards are contained in paragraph 3-3010 of this section.

3-3007 DIGITAL ELECTRONIC SIGNATURES. Digital signatures are electronic signatures that incorporate encryption and decryption technology. Digital signatures that use this technology are typically the most secure because of the controls that are inherent with the technology itself.

A. Digital Cryptography. Digital signature technology is based on Public and Private Key Infrastructure (PKI) cryptography. PKI cryptography is a class of cryptographic algorithms which require two separate keys, one of which is secret (private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text and to create a digital signature. To ensure the authenticity of a digital signature, PKI must incorporate the use of a digital certificate to authenticate the signatory's identity. A digital certificate is issued by a trusted third party to establish the identity of the

signatory. The third party who issues the digital certificate is known as a certificate authority (CA). The CA assumes the responsibility and liability of vouching for an individual's identity.

1) Public Key. A public key in a digital signature encrypts the digital signature itself and essentially converts it to a series of numbers and letters that are nearly impossible to duplicate. The encrypted data in a digital signature public key can be accessed by anybody; hence the term "public" key. However, only the individual with the private key can turn the encrypted data into a digital signature. Examples of public keys include Smartcards, Digital Tokens, Access Badges, or a user ID.

2) Private Key. A private key is used by the individual signatory to decrypt the public key data and turn it into a digital signature. Examples of private keys are unique user name/password/access code combinations. The signatory must keep the private key secret and stored in a protected environment.

3) Digital Certificate and CA. The digital certificate verifies the signatory. A digital certificate is like an identification card. The CA verifies the signatory's identity and issues the certificate.

B. Controls. Digital electronic signatures that use PKI and incorporate digital certificate authentication contain controls that ensure the authenticity of the signature. This technology also ensures the signature is permanently embedded in the document, record, or data in such a way as to render the content unalterable without a new signature.

3-3008 ELECTRONIC SIGNATURE PROCESS. A certificate holder who desires to use electronic signatures must have a definitive process that ensures all of the elements that comprise a valid electronic signature, in accordance with the FAA standards, are present. When evaluating a certificate holder's electronic signature process, PIs and ASIs should be able to verify that the process includes all of the required elements. The burden of proof in this case is on the certificate holder, who must be able to show the PI/ASI that the certificate holder's electronic signature process incorporates all of the required elements.

A. Signature Uniqueness. An electronic signature is only valid if it is unique to the individual signatory. An electronic signature process must have a means to ensure the uniqueness of an electronic signature. The process must ensure the electronic signature is difficult to duplicate.

B. A Means to Convey the Signatory's Intent to Sign. An electronic signature process should prompt the signatory before the individual affixes his or her signature. The electronic signature block should contain a word or statement that definitely conveys the signatory's intent to affix his or her signature. Examples of statements that verify or convey the intent of an individual to affix his or electronic signature include, but are not limited to:

- "Signed by,"
- "Certified by,"
- "Instructor's signature/certification,"
- "Signature,"

- “Authorized by,”
- “Signatory,” and
- “Authentication.”

C. Notification of Signed Record or Document. An electronic signature process should notify the signatory that the signature has been affixed.

D. Signature Association. An electronic signature process must ensure that each electronic signature is attached to, or logically associated with, the record or document being signed. There are two aspects to this requirement:

1) Scope of Information. The scope of information being affirmed with an electronic signature must be clear to the signatory and to subsequent readers of the record or document. Handwritten documents typically place the signature line close to the information to identify those items affirmed by the signatory. This is the preferable method of clearly identifying the information being attested to by the signature. In an electronic signature environment, the signer must have an opportunity to review the record before signing it. This is necessary to ensure the signer clearly understands the scope of what he or she is signing. It is also critical that the electronic signature process be established in a manner that ensures the signer’s electronic signature is applied only to what the signer is actually able to review.

2) The Electronic Signature Must Be Linked to the Record or Document. Each electronic signature must be permanently linked to the record or document being signed. An electronic signature process must ensure that each record or document that contains an electronic signature is stored in such a manner that permanently associates and/or attaches the electronic signature to the record or document that was signed.

E. Retrievable and Traceable. An electronic signature process must provide positive traceability to the individual who signed the document or record. Each person that signs an electronic record or document should be able to identify and retrieve the documents or records that contain his or her electronic signature.

F. Permanent and Unalterable. An electronic signature process must ensure that each signature is permanently affixed to the document or record in its original form and content at the time it was signed. The information contained in the record or document must be unalterable without a new signature to validate the alteration.

G. Security Protocols and Prevention of Unauthorized Access and Modifications. A certificate holder’s electronic signature process must be secure and must prevent unauthorized access to the system that affixes the signature to the intended documents or records. The process must ensure that only the intended signatory can affix his or her signature and must prevent unauthorized individuals from certifying required documents, such as airworthiness or dispatch releases. The process must prevent modifications to information/data or additional entries to records or documents without requiring a new signature. Additionally, the process should contain restrictions and procedures to prohibit the use of an individual’s electronic signature when the individual leaves or terminates employment.

H. Correctable. An electronic signature process should include a means for a certificate holder to correct records or documents that were electronically signed in error as well as those documents where a signature is properly affixed but the information or data is in error. An electronic signature should be invalidated any time a superseding entry is made to correct the record or document. The information or signature being corrected should be voided but remain in place. The new information and/or signature should be easily identifiable.

I. Archivable. An electronic signature process must have a means of safely archiving electronically signed documents.

J. Control of Private Keys and Access Codes. A digital electronic signature process must ensure the private key or access to the electronic system that affixes the signature is under the sole custody of the signatory at all times.

K. Policies and Procedures. Each certificate holder that uses electronic signatures must have policies and procedures that address each requirement listed in paragraphs 3-3006, 3-3007 (for digital electronic signatures), and 3-3008 of this section. The policies and procedures must be part of the certificate holder's manual system. In addition, the policies and procedures should include the following:

1) Regulatory Compliance. Procedures should address how the electronic signature process ensures compliance with the 14 CFR regulatory requirements as they apply to records and documents that require signatures.

2) A Description of the Electronic Signature Process. A description of the electronic signature process must be included in the certificate holder's manual. For parts 91K, 121, 125 and 135, each electronic signature process must be identified by a revision number and date. For a new unrevised process, a certificate holder may identify the revision number as "0" or "Original." A reference to the process revision number and date, as well as the manual that contains the description of the electronic signature process, will be part of the OpSpec A025 authorization. For those certificate holders who are not required to have manuals (e.g., part 135 single pilot and part 141), a standalone electronic signature process document is an acceptable alternative, provided it is an official document maintained by the certificate holder.

a) **How the Process is Used.** The description should explain how electronic signatures will be used and how electronic signatures are applied throughout the certificate holder's operation (e.g., dispatch releases, training records, airworthiness releases, and maintenance actions).

b) **Hardware and Software Capabilities.** The process description should include the hardware to be used and the software capabilities.

3) Responsible Personnel. Policies and procedures should identify the certificate holder's personnel who have the authority and overall responsibility for the integrity and security of the electronic signature process and for controlling access to the computer software/application used in the process. Policies and procedures should also identify the persons with the authority and responsibility for modifying, revising, and monitoring the electronic signature process, as well as ensuring the process is followed by all appropriate personnel.

4) Defined Users. Policies and procedures should identify the authorized users of the electronic signature process. This includes identifying each user's role in the process along with the records or documents each user is authorized to sign electronically.

5) Training and User Instructions. A certificate holder's policies and procedures should include any training and instructions necessary to ensure authorized users understand how to access and properly apply the electronic signature process. Policies and procedures should include how the certificate holder will provide users with any changes to the process.

6) System Support. Policies and procedures should address system support of any computer hardware or software that is part of the electronic signature process.

7) Quality Control (QC) and Auditing. Policies and procedures should include QC and auditing measures that ensure all of the requirements for electronic signatures continue to be met. The process should include unauthorized event recognition, which includes actions to be taken by the certificate holder upon discovery of an attempt by an unauthorized individual to use an electronic signature.

8) Process Changes Require FAA Acceptance Prior to Implementation. A certificate holder's electronic signature process policies and procedures should address how the certificate holder will submit changes to the electronic signature process to the FAA for acceptance. For parts 91K, 121, 125 and 135 operations, certificate holders will be required to identify changes to the process by revision number and date. This information will become part of the OpSpec A025 authorization. For all operations to which this section applies, revisions to the electronic signature process must be included in the manual or official document containing the electronic signature process description.

3-3009 ACCEPT AN ELECTRONIC SIGNATURE PROCESS AND AUTHORIZE THE USE OF ELECTRONIC SIGNATURES. PIs and ASIs will follow the FAA's general process for approval and acceptance contained in Volume 3, Chapter 1, along with the information contained in subparagraphs 3-3009A through D below.

NOTE: The process described in this paragraph is not required for parts 61, 63, 65, 91 (excluding 91K), 129, 137, or 183.

A. Review and Evaluate the Application. Certificate holders will submit their application for acceptance of an electronic signature process to their CHDO. The application medium (e.g., paper, electronic file, etc.) must be acceptable to both the applicant and the FAA. The PIs or ASIs with oversight responsibility of the certificate holder will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The PIs will include inspectors with the appropriate expertise (e.g., an ASI—Aircraft Dispatcher (ASI-AD) or cabin safety inspector (CSI)) in the review process. If the PIs or other certificate management personnel identify deficiencies in the application package, the certificate holder must correct all of the deficiencies before the PIs/ASIs accept the application package. The application package must include at least the following information:

1) Letter of Intent. The application must contain the certificate holder's letter of intent to use electronic signatures.

a) **Estimated Date of Implementation.** The letter must include the estimated date on which the certificate holder would like to begin using electronic signatures.

b) **Primary Point of Contact (POC).** The letter must include the certificate holder's primary POC for the electronic signature application process.

2) A Description of the Proposed Electronic Signature Process. The electronic signature process description must address all of the requirements contained in paragraphs 3-3006, 3-3007 (for digital electronic signature), and 3-3008 of this section.

3) The Documents and/or Records that will Contain an Electronic Signature. The application must state specifically which documents or records the certificate holder desires to contain an electronic signature.

4) Manual Containing the Electronic Signature Process. The certificate holder must include a copy of the manual(s) (or document for operations that do not require a manual) that contains the electronic signature process description.

B. Demonstration of the Process. After accepting the application package, the PIs/ASIs should have the certificate holder demonstrate the electronic signature process. The demonstration should include the following:

1) Hardware and Software Capabilities. The certificate holder should demonstrate the actual electronic signing of a document.

2) Security Protocols and Prevention of Unauthorized Access and Modification. The certificate holder should demonstrate the following:

a) How the electronic signature process prevents unauthorized personnel from signing a document or record.

b) How the process prevents anybody other than the intended signatory to affix his or her signature.

c) How modifications to a signed document or record are prevented without a new signature.

d) How the signature is permanently affixed to the document or record being signed.

3) QC Procedures. The certificate holder should demonstrate its QC procedures for ensuring the security and authenticity of electronic signatures.

C. Accept the Process and Authorize the Use of Electronic Signatures. If the certificate holder successfully completes the application and demonstration phase, the CHDO may accept the certificate holder's electronic signature process. For part 91K, 121, 125, 133, 135, 141, 142, 145, or 147, the vehicle for accepting a certificate holder's electronic signature process and authorizing a certificate holder to use electronic signatures, is OpSpec A025. PIs and

ASIs with the authority to sign OpSpecs will indicate acceptance and authorization of the electronic signature process by making the appropriate selections in OpSpec A025, signing the OpSpec and issuing it to the certificate holder. The PI's or ASI's signature conveys the FAA's acceptance of the process for each type of signature listed in A025. When the PI or ASI issues A025 in WebOPSS, the certificate holder is authorized to use those electronic signatures listed as of the effective date of the active OpSpec. This date also signifies the effective date of FAA acceptance. Guidance on how to populate A025 is located in Volume 3, Chapter 18, Section 3. PIs/ASIs must review this guidance prior to authorizing the use of the electronic signatures in the A025 template.

D. Reject an Inadequate Process. If the CHDO determines the certificate holder's electronic signature process is inadequate for any reason, the CHDO will reject the application in writing and provide an explanation to the certificate holder.

3-3010 ELECTRONIC RECORDKEEPING SYSTEM REQUIREMENTS. This paragraph provides the FAA's standards for electronic records and lists the elements that are required in an electronic recordkeeping system. PIs and ASIs should generally understand the difference between a recordkeeping system and an information management system. A recordkeeping system stores and preserves evidence of a particular event. A system that collects and displays information that does not preserve the evidence of an event is not a recordkeeping system; it is an information management system. An electronic recordkeeping system must incorporate all of the elements that constitute a valid record and must meet the following requirements:

A. FAA Standards for Electronic Records. An electronic record must provide equivalent or better, data integrity, accuracy, and accessibility to what would otherwise be provided by a paper record. In general, a record preserves the evidence of an event. It must contain enough information to clearly depict the event that took place. A record must contain at least the following information:

- 1) The type of event took place (e.g., training, maintenance performed, signing of a release, conduct of a flight, etc.).
- 2) For a training event, information that shows compliance with regulatory requirements, such as the name of the course module or subject, the number of hours of instruction, whether the student passed or failed, etc.
- 3) When the event took place (e.g., the date and time (where appropriate)).
- 4) Where the event took place (e.g., the station, training facility, maintenance facility, etc.).
- 5) Who was involved in the event (e.g., crewmember, dispatcher, instructor, mechanic, etc.).
- 6) Aircraft type and registration number for pilot logbook records (when required by regulation).

7) Certification, verification or authentication of the event, such as a signature, where required by regulation.

8) Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model, for maintenance records such as life-limited parts and time-in-service records.

NOTE: More detailed information regarding maintenance recording and recordkeeping requirements is contained in Volume 3, Chapter 31, Sections 5 and 6.

B. Electronic Recordkeeping Systems. Each certificate holder with an electronic recordkeeping system must have policies, procedures, and methods in place that support the use of the system and ensure the integrity of the records maintained on the system. Electronic recordkeeping system procedures must be incorporated into the certificate holder's manual system, along with a description of the system itself. For those certificate holders who are not required to have manuals (e.g., part 135 single pilot and part 141), a standalone electronic recordkeeping system procedures document is an acceptable alternative, provided it is an official document maintained by the certificate holder. Policies, procedures, and system descriptions must address all of the elements outlined in paragraph 3-3010, including all of the subparagraphs contained therein.

1) System Description. The certificate holder's manual (or document for operations that do not require a manual) must contain a detailed description of each electronic recordkeeping system utilized by the certificate holder to maintain and store records required by 14 CFR. A certificate holder may utilize more than one system to maintain various kinds of records. In addition to addressing all of the elements contained in paragraph 3-3010, including all of the subparagraphs contained therein, the system description should include the following:

- a) System facilities, hardware, and software.
- b) Identification of the records maintained and stored on the system. If there is more than one system, a description of each recordkeeping system is required along with the records maintained and stored on each system.
- c) Identification of which electronic records for which the certificate holder will use an authorized electronic signature process.

2) Security. An electronic recordkeeping system must ensure that each record is preserved and cannot be altered. Access to the system must be controlled and password protected. The system must also have the ability to protect confidential information.

3) Authenticity and Prevention of Unauthorized Access or Data Corruption. An electronic recordkeeping system must have a method of ensuring the integrity of each record through appropriate levels of security such as recognition of an electronic signature or other means, which uniquely identify the initiating person as the author of that record. The system must provide for secure access and contain safeguards against unauthorized access. Procedures should include unauthorized event recognition, which includes actions to be taken by the certificate holder upon discovery of an attempt by an unauthorized individual to access and/or make entries into the electronic recordkeeping system.

4) QC and Auditing. An electronic recordkeeping system should have a means to ensure the quality, accuracy, and integrity of the records maintained on the system, as well as any backup to the system. There should be auditing procedures for computer systems and workstations that are part of, or have access to, the electronic recordkeeping system. QC policies and procedures must include at least the following:

a) **Verification of Record Accuracy.** Policies and procedures must include the verification of the accuracy and integrity of records maintained on the recordkeeping system through auditing at regular intervals (e.g., biannually, annually, or in accordance with a certificate holder's training cycle).

b) **Verification of Backup Integrity.** Policies and procedures should include verification of the accuracy and integrity of records maintained on the backup system.

c) **Verification of Changes Requiring Electronic Signature.** Policies and procedures must include verification that any changes made to record data contain a new electronic signature, for those records that contain signatures.

d) **Persons Responsible for Verification.** Policies and procedures must name the person responsible for the QC process and for verification of records.

5) Maintenance Support and Backup Measures. The system should include procedures for maintenance and support that include provisions for electronic system (computer hardware, software, application network, etc.) outages and protect against the loss of record data. The system should also include backup measures to maintain and provide access to records in the event of a system failure. The method of backup may be a separate electronic system, a backup server, or backup drive. Backup can also include media, such as print or CD-ROM, external drive, or other media acceptable to the FAA.

6) Procedures for Making Required Records Available to FAA and National Transportation Safety Board (NTSB) Personnel. A certificate holder must provide its records in a format and manner that is acceptable to the requesting agency. FAA personnel assigned to a certificate holder with an electronic recordkeeping system may request a certificate holder to provide direct access to the electronic system for the purpose of inspecting regulatory records. Providing this direct access to the FAA is voluntary. The FAA will not request direct electronic access to records beyond those that are required by regulation and authorized in A025. It is important to distinguish a certificate holder's voluntary provision of direct access to its electronic recordkeeping system to the FAA from the certificate holder's responsibility to make regulatory

records available to the FAA in accordance with 14 CFR part 119, § 119.59(c). In accordance with this regulation, each employee of, or person used by, the certificate holder who is responsible for maintaining the certificate holder's regulatory records (those required under Title 49 of the United States Code (49 U.S.C.) applicable to the operation of the certificate holder) must make those records available to the Administrator.

7) Training and User Instructions. A certificate holder with an electronic recordkeeping system must provide training and user instructions to persons responsible for entering, maintaining, and retrieving data from the system. Training should include security awareness and system integrity, as well as procedures that are necessary to authorize access to the electronic recordkeeping system. User instructions should include those for FAA personnel who are provided direct access to the system. Acceptable methods of providing training include, but are not limited to: classroom instruction, online or system tutorials, user guides, and simulated problem solving exercises.

8) Persons with Authorized Access. System procedures should address specific access requirements for personnel authorized to make entries into the system. The certificate holder must provide each person with a unique individual access code and password to validate any entry made by the individual.

9) Instructor and Evaluator Access and Certifications. Policies and procedures should address access by designated personnel, such as instructors, check pilots, check Flight Engineers (FE), aircraft dispatcher supervisors, and flight attendant (F/A) supervisors, to electronically enter record information and certify all record entries for which they are responsible. Electronic instructor certifications must meet all of the requirements of a valid electronic signature. The certificate holder may devise a system that requires the validating official to either enter a real-time record into the system or complete a written transmittal document in Portable Document Format (PDF) to be uploaded into the system by the appropriate personnel. If a PDF is used, the document must contain a valid electronic signature of the individual certifying the record. For authentication purposes, the electronic signature must be a permanent part of the electronic record.

10) Responsible Personnel. Policies and procedures should identify the personnel who have the overall responsibility for the integrity and security of the electronic recordkeeping system(s) and who are responsible for controlling access to the system. Policies and procedures should also identify the persons with the authority and responsibility for modifying the electronic record system, as well as those who are responsible for entering data into the system.

11) Transferring Data to Another System. Technological advances may make it desirable or necessary for a certificate holder to update its electronic recordkeeping system or transfer data to a new system. The certificate holder must have policies and procedures that ensure the continued integrity of record data when a certificate holder moves records from one system to another. This could entail running redundant systems for a brief period of time.

12) Continuity of Data between Legacy and Electronic Systems. Any certificate holder should have a method to ensure continuity of data during transition from a legacy system (hardcopy) to an electronic system.

13) Continuity of Data for Outsource Maintenance Providers. Procedures should ensure continuity of record data utilized and maintained by outsource maintenance providers.

14) Maintenance Record Transfer. Procedures should ensure that electronic maintenance records transferred with an aircraft meet the regulatory requirements for record transfer (refer to part 43, § 43.10, and §§ 91.419, 121.380a, and 135.441).

15) Electronic Authentication, Signature, Validation, or Endorsement. Most regulatory records require some kind of validation, such as a signature, certification, endorsement, or authentication. This validation must be a permanent part of any electronic record. To be considered valid, any electronic form of validation, authentication, endorsement, etc., must meet the FAA's standards for electronic signatures, and the certificate holder must have the authority to use electronic signatures in its OpSpec A025. See paragraph 3-3006 for FAA standards for electronic signatures.

C. Changes to the System Require FAA Approval or Acceptance Prior to Implementation. A certificate holder's policies and procedures should include details of when revisions to the electronic recordkeeping system will be submitted for approval or acceptance (depending on the regulatory requirement) prior to implementation. This includes new versions of system software. Software version numbers will be included in the OpSpec A025 authorization for parts 91K, 121, 125, and 135. For all operations to which this section applies, changes to the electronic recordkeeping system must be included in the manual or official document containing the electronic recordkeeping system description.

3-3011 ACCEPT OR APPROVE AN ELECTRONIC RECORDKEEPING SYSTEM. PIs and ASIs will follow the FAA's general process for approval and acceptance contained in Volume 3, Chapter 1, along with the information contained in subparagraphs 3-3011A through D below. Information on whether or not an electronic recordkeeping system requires FAA approval versus acceptance is contained in paragraph 3-3004 toward the beginning of this section.

NOTE: The process described in this paragraph is not required for parts 61, 63, 65, 91 (excluding 91K), 129, 137, or 183.

A. Review and Evaluate the Application. Certificate holders will submit their application for acceptance or approval of an electronic recordkeeping system to their CHDO. The application medium (e.g., paper, electronic file, etc.) must be acceptable to both the applicant and the FAA. The PIs or ASIs with oversight responsibility of the certificate holder will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The PIs will include inspectors with the appropriate expertise (e.g., an ASI-AD or CSI) in the review process. If the PIs or other certificate management personnel identify deficiencies in the application package, the certificate holder must correct all of the deficiencies before the PIs/ASIs accept the application package. The application package must include at least the following information:

1) Letter of Intent. The application must contain the certificate holder's letter of intent to use an electronic recordkeeping system.

a) **The Name of the Electronic System(s).** The letter must include the kinds of records along with the name of the electronic system to be used to maintain the records. There may be more than one system required to maintain various kinds of records.

b) **Estimated Date of Implementation.** The letter must include the estimated date on which the certificate holder would like to implement the electronic recordkeeping system.

c) **Primary POC.** The letter must include the certificate holder's primary POC for the electronic recordkeeping system application process.

2) A Description of the Proposed Electronic Recordkeeping System(s). The electronic recordkeeping system description must address all of the requirements contained in paragraph 3-3010 of this section, including the subparagraphs contained therein, and include a description of the system facilities, hardware, and software. Software version numbers must be included.

3) The Records That Will be Maintained in the System. The certificate holder must state specifically which records the certificate holder intends to maintain and access via the electronic recordkeeping system. The application should include a sample of each record type.

4) The Data Backup. The application must describe the details of the certificate holder's data backup system.

5) Access and Security Procedures. The application must include information regarding access and security procedures.

6) Electronic Signature Processes. The application must include a description of any electronic signature process associated with each record category.

B. Demonstration of the System. After accepting the application package, the PIs/ASIs should have the certificate holder demonstrate the electronic recordkeeping system prior to accepting or approving the system and authorizing the certificate holder to use it. The demonstration should include the following:

1) User Access. The certificate holder should demonstrate how to securely access the system.

2) Security Protocols and Prevention of Unauthorized Access and Record Modification. The certificate holder should demonstrate how the system prevents unauthorized access or modifications to the records maintained on the system.

3) Record Entry. The certificate holder should demonstrate how a record is entered into the system.

4) QC Procedures. The certificate holder should demonstrate the procedures for ensuring the quality and integrity of each record maintained on the system.

C. Accept or Approve the System and Authorize its Use. If the certificate holder successfully completes the application and demonstration phase, the CHDO may accept or approve the certificate holder's electronic recordkeeping system.

1) Approval Required. If the system is used to maintain the crewmember and dispatcher records required by parts 121 or 125, then using an electronic recordkeeping system for those records requires FAA approval. The recordkeeping system description, as well as all of the associated policies and procedures, is subject to FAA approval. The CHDO will use A025 as the method of approval. To accomplish this, the principal operations inspector (POI) or delegated ASI with OpSpec signature authority will populate the appropriate table in A025, sign the OpSpec, and issue it to the certificate holder. The POI's or ASI's signature conveys the FAA's approval. When the POI or ASI issues A025 in WebOPSS, the certificate holder is authorized to use the electronic recordkeeping system(s) listed as of the effective date of the active OpSpec. This date also signifies the effective date of FAA approval. Instructions on how to correctly populate A025 are contained in Volume 3, Chapter 18, Section 3. POIs and ASIs must review these instructions prior to approving and authorizing the use of an electronic recordkeeping system. Any changes to the system or associated policies and procedures will require a new approval.

2) Acceptance Required. If the system requires FAA acceptance, the CHDO will convey acceptance in the same manner as an approval. For operations in accordance with parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147, the method for accepting an electronic recordkeeping system and authorizing a certificate holder to use it is OpSpec A025. PIs and ASIs will indicate acceptance and authorization of the electronic recordkeeping system by populating the appropriate table in A025, signing the OpSpec, and issuing it to the certificate holder. The PI's or ASI's signature conveys the FAA's acceptance. When the PI or ASI issues the OpSpec in WebOPSS, the certificate holder is authorized to use the electronic recordkeeping system(s) listed as of the effective date of the active OpSpec. This date also signifies the effective date of FAA acceptance. Instructions on how to correctly populate A025 are contained in Volume 3, Chapter 18, Section 3. PIs and ASIs must review these instructions prior to accepting and authorizing the use of an electronic recordkeeping system in the A025 template.

D. Reject an Inadequate System. If the CHDO determines the certificate holder's electronic recordkeeping system(s) is inadequate for any reason, the CHDO will reject the application in writing and provide an explanation to the certificate holder.

3-3012 ELECTRONIC MANUALS. An electronic manual must provide equivalent or better, data integrity, accuracy, and accessibility to what would otherwise be provided by a printed manual. The content of each electronic manual must be clearly identifiable and viewable by the user and must correlate and be comparable to what would be available in a printed version of the manual. Like printed manuals, electronic manuals must provide instructions and information necessary to allow personnel concerned to perform their duties and responsibilities with a high degree of safety. An electronic manual should contain the elements that generally comprise a printed manual. These elements typically include:

- The manual title;
- Revision control pages or sections from which the user can readily determine whether the manual is current;
- List of effective pages or sections;
- Indication of FAA approval (e.g., signature or stamp) for those manuals or manual sections that require FAA approval;
- Chapter numbers;
- Chapter headings;
- Section numbers;
- Topic headings;
- Page numbers;
- Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (when applicable for MEL and maintenance purposes); and
- The person with the authority and responsibility for manual content.

3-3013 ELECTRONIC MANUAL SYSTEM. An electronic system for delivering manual content must comply with regulatory requirements for currency, availability, and distribution to the appropriate personnel. Each certificate holder with an electronic manual system must have policies and procedures in place that support the use of the system and ensure the integrity of the manual content maintained and distributed via the system. Electronic manual system procedures must be incorporated into a certification holder's manual system. Each electronic manual system must provide the following:

A. Currency. Each certificate holder's electronic manual system must have a method of keeping each manual current and up to date.

B. Access, Availability, and Distribution. Each electronic manual system must provide distribution (also known as furnish) and/or access to manuals to the appropriate personnel in a form and method acceptable to the Administrator. Regulatory requirements for availability and distribution of manuals vary subtly according to regulatory part. Some regulations, such as those related to MELs, require a certificate holder provide access to a manual, as opposed to distributing it. PIs and ASIs with oversight responsibility must review the appropriate requirements for manuals, as they apply to the regulatory part under which a certificate holder is conducting its operations, repairs, and/or training.

C. MEL Direct Access Approval Requirement – Parts 91K, 121, 125, and 135.

A certificate holder who conducts parts 91K, 121, 125, or 135 operations requires FAA approval to provide flightcrews with direct access to the MEL in any means or format other than printed. The FAA will only approve electronic access to an MEL if the MEL is part of a certificate holder's electronic manual system. A certificate holder desiring FAA approval to electronically distribute its MEL must list the MEL in the master manual or document that describes the electronic manual system and lists each manual in the system. The master manual or document is discussed later in this section. The FAA will approve electronic access to an MEL by populating the appropriate table in OpSpec A025. The PI's signature on the OpSpec conveys the FAA's approval. Information regarding the population and issuance of A025 is located in Volume 3, Chapter 18, Section 3.

D. FAA and NTSB Access. Each certificate holder must furnish copies of its manuals to appropriate FAA personnel. In addition, each certificate holder must provide any requested information to the NTSB in the event of an accident or incident. When a certificate holder is required to provide manuals or manual information to the FAA or NTSB, whenever possible, it should be provided in the desired format of the requesting agency. FAA personnel assigned to a certificate holder with an electronic manual system should encourage the certificate holder to provide direct access to the system by the appropriate CHDO personnel.

E. Responsible Personnel. Each electronic manual system description should include the person(s) with the authority and responsibility for maintaining the system, implementing, modifying, revising, and monitoring the electronic manual software and ensuring the overall integrity of the content of manuals that are part of the system.

F. Prevention of Unauthorized Access and Data Corruption. Manual system computer hardware and software must prevent unauthorized access and/or modification to electronic manual content. The certificate holder should have procedures for reporting and analysis of any known unauthorized access attempts.

G. Storage and Retrieval. Computer hardware and software systems must be able to store and retrieve the manual's content under conditions of normal operation and use.

H. Functionality. Manual users should be able to easily access, navigate, and retrieve manual content via computer or comparable device. Manual users should be able to print any information contained in an electronic manual whenever necessary.

NOTE: Once printed, content from an electronic manual could be less current than what is maintained on the electronic manual system.

I. Revision Control. A certificate holder's electronic manuals should be easy to revise. The electronic manual system should include revision control procedures for making revisions (incremental, temporary, and scheduled) in a timely manner. Procedures should include the accomplishment of revisions by personnel to whom manuals are issued. The revision control procedures should address at least the following:

1) Communication of Revision Information. Procedures should include the method of communicating revision information, similar to what would be provided for a paper manual revision. Revision information should provide the revision content, effective date, and any instructions required for ensuring the revision is uploaded or incorporated into the electronic manual. Revision information should allow the user the ability to compare the current revision to the previous version or it should explain the effect of the change. Changes under the revision should be readily apparent to the user. An example of this would be change bars. Each electronic manual should contain a revision control page or section from which the user can readily determine whether the manual is current.

2) Revision Status of Each Manual Page. Each page of a manual should contain the date of the latest revision for that particular page. For part 121 operations, this is required by § 121.135(a)(3). If an electronic manual is distributed via a device that displays the manual in a continuous flow format, as opposed to page-by-page, then each section or block of information displayed on the device must contain the date of latest revision.

3) Date and Time Stamp of Printed Information. When information from an electronic manual is printed, there should be a means to identify the date and time of printing. This ensures the currency of information by allowing the manual user to compare the date of the printed information with the date of the information contained in the electronic manual system. Printed information that has the same date, but differs from the information contained in the electronic manual, would indicate that the manual content was printed before the manual was updated later that day.

4) User Responsibility for Current Information. Users of electronic manuals who need or elect to print material (data, information, instructions, procedures, etc.) from the electronic manual must ensure the printed information is the most current available prior to use. Users should discard printed manual information after using it to ensure printed information does not become outdated.

5) Distribution and Submission of Electronic Revisions to the FAA.

a) Revision control procedures should include the certificate holder's method of distributing electronic revisions to the FAA.

b) When a particular manual requires FAA approval or acceptance, the certificate holder's procedures should explain how the certificate holder will submit an electronic revision to the FAA for approval or acceptance of the revision content.

J. Special Considerations in Displaying Information. Information retrieved from an electronic manual could be displayed in a format that differs from what would appear on paper. The display format could even vary by user. For example, the display of manual content could be different for pilots on the flight deck of an aircraft versus what is displayed to ground personnel at a computer workstation. This could occur for reasons such as screen resolution, software application, or authorized display device. Information displayed on any authorized device on the flight deck must correlate to information displayed at an authorized computer workstation or authorized portable device. Additionally, any information displayed should be easily traceable to and comparable to the source document. The most important point is that the electronic manual content must remain the same regardless of the display format or device. Any displayed manual information must be identical in content for all users.

K. Data Archiving. An electronic manual system should have a method of archiving technical and procedural data superseded by revision. A certificate holder should archive earlier versions of manuals to provide for future needs to duplicate, regenerate, or reconstruct instructions.

1) The Importance of Historical Data. Archived historical data is particularly important for the following reasons:

- a) To trace aircraft repair information or reconstructing maintenance instructions.
- b) To evaluate normal and abnormal flight deck (cockpit) checklist procedures.
- c) For training purposes.
- d) For investigation purposes in the event of an accident, incident, or occurrence.

2) Preservation of Archived Data. An electronic manual system must have procedures to ensure the integrity of the archived technical and procedural data. These procedures should include at least:

- a) A method of ensuring that no unauthorized changes can be made.
- b) A method or medium that minimizes the deterioration of data.
- c) A method to protect the archived data against hazards and natural disasters.

L. Transferring Data to Another System. Technological hardware or software advances may make it desirable and/or necessary for a certificate holder to update its electronic manual system. When transferring manual data from one electronic system or application to another, certificate holders should ensure that data integrity is maintained during transfer. This includes ensuring that archived information remains intact. This could entail running redundant systems for a brief period of time.

M. Backup Method. A certificate holder that uses an electronic manual system must have a backup method of maintaining, distributing, or otherwise providing access to manuals in case of system failure. The backup method may be a separate electronic system; a backup server to the authorized system; backup media such as print or CD-ROM; or other method acceptable to the FAA.

N. System Maintenance and Support. Each certificate holder's electronic manual system should include maintenance and support function that identifies hardware and software failures within the system. System maintenance and support should include provisions for system outages and for switching over to the backup method described in subparagraph 3-3013M above.

O. QC. Each electronic manual system must have QC that ensures the integrity of the data contained in each electronic manual.

P. Master Manual for Parts 91K, 121, 125, and 135. An electronic manual system used in operations under parts 91K, 121, 125, and 135 must include a master manual that describes the electronic manual system and lists each manual maintained and distributed via the system. (A part 135 certificate holder authorized by OpSpec A040 as a Single Pilot Operator who elects to have a manual and maintain/distribute it electronically may list that manual as

being the master manual for the purposes of A025.) The master manual is what the PI will reference when accepting the electronic manual system and authorizing its use in OpSpec A025. The master manual must include at least the following:

1) Description of the Electronic Manual System. The electronic manual system description should include the methods for distribution and/or access to manual(s) (including manual revisions and replacements) by the appropriate personnel.

2) Delivery Media. An electronic manual system description must include an explanation of the media by which manuals will be distributed to required personnel.

3) Personnel with Authority and Responsibility. The master manual must list the certificate holder's personnel who have the overall authority and responsibility for maintaining the electronic manual system.

4) Listing of Manuals—Certificate Holders with Large and Complex Manual Systems. For a certificate holder with a large and complex manual system that contains numerous manuals, it is acceptable to list the kinds of manuals, instead of listing each manual, provided all of the particular kinds of manual are maintained and distributed via the electronic manual system. For example, list: "All Ground Operations Manuals," "All Maintenance Manuals," or "All Training Program Manuals."

Q. Description of the Electronic Manual—Part 133 and 145. For electronic manuals used in parts 133 and 145, a description of how each electronic manual is displayed, maintained, revised and distributed should be included in the certificate holder's manual system. The description must also include an explanation of the media by which manuals will be distributed to required personnel.

R. Training and User Instructions. Each certificate holder must provide training and instructions to users of the electronic manual system. The scope and complexity of the training may vary depending on an individual's duties and responsibilities. Training should include security awareness and computer system (hardware, software, application, network, etc.) integrity. Acceptable methods of providing training include, but are not limited to, classroom instruction, online or system tutorials, or user guides.

S. Changes to the Electronic Manual System Require FAA Acceptance Prior to Implementation. Policies and procedures should address how the certificate holder will submit changes to the electronic manual system to the FAA for acceptance. For parts 91K, 121, 125, and 135, changes to the electronic manual system must be documented through revision to the master manual containing the electronic manual system description. The master manual revision number and date will be included in the OpSpec A025 authorization.

3-3014 ACCEPT AN ELECTRONIC MANUAL SYSTEM. PIs and ASIs will follow the FAA's general process for approval and acceptance contained in Volume 3, Chapter 1, along with the information contained in subparagraphs 3-3014A through D below.

NOTE: The process described in this paragraph is not required for parts 61, 63, 65, 91 (excluding 91K), 129, 137, 141, 142, 147, or 183.

A. Review and Evaluate the Application. Certificate holders will submit their application for acceptance of an electronic manual system and/or approval of an electronic MEL to their CHDO. The application medium (e.g., paper or electronic file) must be acceptable to both the applicant and the FAA. The PIs or ASIs with oversight responsibility of the certificate holder will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The PIs will include inspectors with the appropriate expertise (e.g., an ASI-AD or CSI) in the review process. If the PIs or other certificate management personnel identify deficiencies in the application package, the certificate holder must correct all of the deficiencies before the PIs/ASIs accept the application package. The application package must include at least the following information:

1) Letter of Intent. The application must contain the certificate holder's letter of intent to use an electronic manual system.

a) **Estimated Date of Implementation.** The letter must include the estimated date on which the certificate holder would like to implement the electronic manual system.

b) **Primary POC.** The letter must include the certificate holder's primary POC for the electronic manual system application process.

2) Master Manual or Document for Parts 91K, 121, 125, and 135. An application to use an electronic manual system for part 91K, 121, 125, or 135 must include a copy of the proposed master manual as described in subparagraph 3-3013P.

3) A Description of the Proposed Electronic Manual—Parts 133 and 145. An application to use an electronic manual for parts 133 and 145 must include a description of the electronic manual as described in subparagraph 3-3013Q.

4) Manuals Included in the System. The application must state specifically which manuals the certificate holder intends to maintain and distribute via the electronic manual system.

a) Flight operations manuals by title.

b) Ground operations manuals by title.

c) Maintenance manuals by title.

d) Training program manuals by title.

e) Electronic MELs.

f) General policy manuals by title.

g) User manuals (e.g., flight planning system and other hardware/software applications) by title.

5) Distribution to the FAA. The certificate holder must provide a copy of the electronic manuals to the CHDO and provide an explanation of how revisions and future electronic manuals will be distributed to the FAA.

6) Electronic Access to an MEL. Parts 91K, 121, 125, and 135 require a certificate holder or program manager to have FAA approval and OpSpec authority to provide access to an MEL via electronic means. Certificate holders desiring to provide electronic access to an MEL must specify that in the application and include details on how electronic access will be provided.

B. Demonstration of the System. After accepting the application package, the PIs/ASIs should have the certificate holder demonstrate the electronic manual system prior to accepting the system and authorizing the certificate holder to use it. The demonstration should include the following:

1) Hardware and Software Capabilities. The certificate holder should demonstrate how to use the hardware and software by performing simple tasks within the system.

2) Distribution and Availability. The certificate holder should demonstrate how the manuals will be distributed or made available (depending upon the regulatory requirement) to required personnel electronically.

3) Information Access Capabilities. The certificate holder should demonstrate how to access manual content via the electronic system.

4) Prevention of Unauthorized Modification. The certificate holder should demonstrate how the system prevents unauthorized modifications to manual content.

5) Revision Capabilities. The certificate holder should demonstrate how revisions are posted to electronic manuals.

C. Accept the System and Authorize its Use. If the certificate holder successfully completes the application and demonstration phase, the CHDO may accept the certificate holder's electronic manual system. For operations in accordance with parts 91K, 121, 125, 133, 135, and 145, the vehicle for accepting an electronic manual system and authorizing a certificate holder to use it is OpSpec A025. The A025 authorization for electronic manuals is not required for other parts under 14 CFR. The PI or ASI with OpSpec signature authority will indicate acceptance and authorization of the electronic manual system by making the appropriate entries in OpSpec A025, signing the OpSpec and issuing it to the certificate holder. The PI's or ASI's signature on the OpSpec conveys the FAA's acceptance. When the PI or ASI issues A025 in WebOPSS, the certificate holder is authorized to use the electronic manual system (or manuals, depending on the regulatory part and the OpSpec template) listed as of the effective date of the active OpSpec. This date also signifies the effective date of FAA acceptance. If a certificate holder's MEL is included in the electronic manual system, the PI/ASI will also approve electronic distribution of the MEL by populating the appropriate table, signing the OpSpec, and issuing it to the certificate holder. The PI's or ASI's signature on the OpSpec also conveys the FAA's approval to distribute its MEL electronically. Guidance on how to populate A025 is

located in Volume 3, Chapter 18, Section 3. PIs/ASIs must review this guidance prior to authorizing the use of the electronic manual system in the template.

D. Reject an Inadequate System. If the CHDO determines the certificate holder's electronic manual system(s) is inadequate for any reason, the CHDO will reject the application in writing and provide an explanation to the certificate holder.

3-3015 WITHDRAW THE AUTHORITY TO USE AN ELECTRONIC MANUAL SYSTEM, ELECTRONIC RECORDKEEPING SYSTEM, OR ELECTRONIC SIGNATURE.

A. FAA Initiated. At any time the FAA determines there are inadequacies in a certificate holder's electronic signature process, electronic recordkeeping system, or electronic manual system, the following actions are required:

1) Inform the Certificate Holder. The appropriate PI or ASI with oversight responsibility will inform the certificate holder in writing and provide the reasons why the system or process is inadequate. The letter informing the certificate holder must include a timeframe during which the certificate holder may correct the inadequacies. The timeframe will be no less than 7 calendar-days and will not exceed 30 calendar-days.

2) Withdraw Authority in Accordance with § 119.51(b) if the Certificate Holder Fails to Correct Inadequacies – Parts 121, 125, and 135. If the certificate holder fails to correct the inadequacies within the requisite amount of time, the CHDO will follow the process outlined in § 119.51(b) to amend the certificate holder's OpSpecs by withdrawing all or a portion of the authority to use electronic signatures, an electronic recordkeeping system, or electronic manual system from A025. The authority withdrawn will depend on the applicable inadequacies.

3) Withdraw Authority if a Certificate Holder Fails to Correct Inadequacies – Parts 91K, 133, 141, 142, 145, and 147. If a certificate holder fails to correct the inadequacies within the requisite amount of time, the CHDO will follow an equivalent process to what is required by § 119.51(b).

B. Certificate Holder Initiated. If a certificate holder elects to discontinue using an electronic signature process, electronic recordkeeping system, or electronic manual system, the certificate holder must inform the appropriate PI or ASI by letter. Once informed, PIs of certificate holders who are issued A025 (parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147) will withdraw the authority as appropriate by removing it from A025. The CHDO will retain the letter from the certificate holder for at least 5 years after withdrawing the authority. This time period is in accordance with the current edition of FAA Order 1350.14, Records Management, Records Disposition Reference Table, Items 8300 and 8400. The Records Disposition Reference Table can be accessed at:

http://www.faa.gov/about/initiatives/records/policy/media/retention_schedule.pdf.

1) Discontinue Electronic Signatures.

a) The letter from the certificate holder must include the projected date the certificate holder intends to discontinue using the electronic signatures.

b) The letter must contain a description of how the certificate holder intends to transition from using electronic signatures to using traditional pen-and-ink signatures.

c) The letter must contain a description of how electronically signed documents and records will be reproduced and retained in accordance with the requirements of 14 CFR in hardcopy form.

d) If an electronic signature is used in conjunction with electronic recordkeeping, then the electronic signature portion of the recordkeeping system must be removed.

2) Discontinue Electronic Recordkeeping System.

a) The letter from the certificate holder must include the projected date the certificate holder intends to discontinue using the electronic recordkeeping system.

b) The letter must contain a description of how the certificate holder intends to transition from electronic records to paper. The description must include how the certificate holder intends to ensure the content of the paper records exactly matches the electronic content, including having the required signatures.

c) The letter must include the estimated date the paper records will be ready for FAA review.

3) Discontinue Electronic Manual System.

a) The letter from the certificate holder must include the projected date the certificate holder intends to discontinue using the system and provide hardcopy manuals when required by the appropriate 14 CFR part.

b) The letter must contain a description of how the certificate holder intends to transition from electronic manuals to paper manuals. The transition description should include procedures for the certificate holder to audit the paper manuals by comparing them to the electronic manuals and reconcile any differences.

c) The letter must include the estimated date the hardcopy manuals will be provided to the CHDO/FSDO.

RESERVED. Paragraphs 3-3016 through 3-3030.