U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals

Date: 6/22/16 **AC No:** 120-78A

Initiated by: AFS-300 **Change:**

This advisory circular (AC), as any AC, is not mandatory and does not constitute a regulation; rather, it provides standards and guidance for electronic signatures, electronic recordkeeping, and electronic manual systems. Electronic recordkeeping systems/programs are used to generate many types of records (e.g., load manifests, dispatch release, aircraft maintenance records, maintenance task cards, pilot training records, flight release, and/or airworthiness release). This AC describes an acceptable means, but not the only means, for a certificate holder to utilize an electronic signature, electronic recordkeeping, and electronic manual systems.



John Barbagallo
Deputy Director, Flight Standards Service

CONTENTS

Paragraph Page

CHAPTER 1. GENERAL INFORMATION....1

1-1. Purpose....1
1-2. Cancellation....1
1-3. Where This AC Can Be Found....1
1-4. Audience....1
1-5. Scope....1
1-6. Background....3
1-7. Definitions....3
1-8. Approval, Acceptance, and Authorization....4

CHAPTER 2. ELECTRONIC SIGNATURES....7

2-1. Electronic Signature....7
2-2. Electronic Signature Process....9
2-3. Electronic Signature Authorization....12

CHAPTER 3. ELECTRONIC RECORDKEEPING....15

3-1. Electronic Records....15
3-2. FAA Standards for Electronic Records....15
3-3. Electronic Recordkeeping System....15
3-4. Electronic Recordkeeping Authorization....18

CHAPTER 4. ELECTRONIC MANUAL SYSTEMS....21

4-1. Electronic Manuals....21
4-2. Electronic Manual System....21
4-3. Electronic Manual Authorization....25

CHAPTER 5. VOLUNTARY DISCONTINUANCE BY CERTIFICATE HOLDER....29

5-1. Voluntary Discontinuance....29

CHAPTER 6. ADMINISTRATIVE....31

6-1. Questions About This AC....31
6-2. Other Related Regulations, Guidance, and Reading Material....31
6-3. Obtaining Reference Material (current editions)....32

APPENDIX 1. SAMPLE LETTER OF INTENT (2 pages)....1

CHAPTER 1. GENERAL INFORMATION

1-1. PURPOSE. This advisory circular (AC) provides "approval" or "acceptance" guidelines for electronic signature, electronic recordkeeping, and electronic manual systems/programs. It is the certificate holder's responsibility to address all Title 14 of the Code of Federal Regulations (14 CFR) parts that apply to their operation(s).

1-2. CANCELLATION. This AC cancels AC 120-78, Acceptance and Use of Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manuals, dated October 29, 2002.

1-3. WHERE THIS AC CAN BE FOUND. Certificate holders and the public may find this AC at: http://www.faa.gov/regulations_policies/advisory_circulars.

1-4. AUDIENCE. This AC applies to the following regulated entities:

- Foreign air carriers or foreign persons operating a U.S.-registered aircraft in accordance with 14 CFR part 129, § 129.14.
- Certificate holders conducting operations in accordance with 14 CFR part 121, 125 (including part 125 Letter of Deviation Authority (LODA) holders), 133, 135, or 137.
- Fractional ownership program managers conducting operations in accordance with 14 CFR part 91 subpart K (part 91K).
- Operators conducting operations in accordance with part 91.
- Airmen certification course operators who provide instruction and evaluation in accordance with 14 CFR part 61, 63, 65, 141, or 142.
- Persons performing airmen certification in accordance with part 61, 63, 65, 141, or 142.
- Individuals performing maintenance or preventive maintenance in accordance with 14 CFR part 43.
- Repair stations operating in accordance with 14 CFR part 145.
- Aviation maintenance technical schools who provide instruction and evaluation in accordance with 14 CFR part 147.
- Organization Designation Authorization (ODA) holders in accordance with 14 CFR part 183 subpart D.

NOTE: For the purposes of the AC, the term "certificate holder" is used to identify the regulated entities identified in paragraph 1-4 of this AC. The scope of this AC is intended for entities regulated by the Federal Aviation Administration's (FAA) Flight Standards Service (AFS) and is not intended to apply to production, design, or manufacturing authority (e.g., type certificate (TC), Supplemental Type Certificate (STC), Parts Manufacturer Approval (PMA), etc.) signature, recordkeeping, and manual requirements established by the FAA's Aircraft Certification Service (AIR).

1-5. SCOPE. Signatures, records, and manuals as discussed in this AC generally apply to the following categories. (This list is not intended to be all inclusive.)

a. Signatures:

- Certification of Training or Qualification;
- Pilot Logbooks;
- Fitness for Duty;
- Flight/Dispatch Release;
- Load Manifests;
- Operational Control Briefing;
- Preflight Risk Analysis Worksheet;
- Maintenance Logbook;
- Airworthiness Release;
- Maintenance Performed; and
- Continuous Airworthiness Maintenance Program (CAMP) Extended Operations (ETOPS) Predeparture 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.).

1-6. 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 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. OMB Circular A-130, Management of Federal Information Resources, provides general guidance for federal organizations regarding the use of electronic signatures in connection with electronic records and electronic transactions. The use of these electronic technologies also supports the goals of the Small Business Paperwork Relief Act of 2002 (SBPRA) (H.R. 327). This AC provides guidelines on meeting the FAA's performance standards developed in accordance with the listed PLs and OMB memorandum.

1-7. DEFINITIONS. The following terms are used in this AC.

a. Authentication. The means by which a system validates the identity of an authorized user. These may include a password, a personal identification number (PIN), a cryptographic key, smart card, etc. These means may be combined (e.g., a cryptographic card and a PIN) for increased confidence in the identity of the system user.

b. Computer-Based Recordkeeping System. A system of record processing in which records are entered, maintained, archived, and retrieved electronically. The term "computer-based recordkeeping system" is synonymous with "electronic recordkeeping system."

c. Data Backup. Use of one of several recognized methods of providing a secondary means for archiving records, separately from the original or primary. This can be used to reconstruct the format and content of electronically stored records in case of loss, failure, or damage to the primary recordkeeping system.

d. Data Verification. A process of ensuring accuracy of data records by systematically or randomly comparing electronic records with manual data entry documents.

e. Digital Signature. Cryptographically generated data that identifies a document's signatory, with date and time. The result of which, when properly implemented, provides the services of original authentication, data integrity, and signer non-repudiation.

f. Electronic Manuals. Certificate holder manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, Internet/Intranet-based, or various other forms of electronic media, to include commercial off-the-shelf portable electronic device (PED) hardware (e.g., laptop, tablet, phone, etc.).

g. Electronic Record. A contract or other record created, generated, sent, communicated, received, or stored by electronic means.

h. Electronic Recordkeeping System. A system of record processing in which records are entered, signed, stored, and retrieved electronically. The term "electronic recordkeeping system" is synonymous with "computer-based recordkeeping system."

i. Electronic Signature. Functionally equivalent to a handwritten signature. The term "electronic signature" means 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.

j. Operations Specifications (OpSpec). Documents created and issued by the FAA through the Web-based Operations Safety System (WebOPSS) are collectively referred to as "Authorizing Documents." For the purposes of this AC, the use of the term "OpSpec" hereafter refers to one or more of the following WebOPSS authorization documents:

(1) Management Specifications (MSpecs). Issued to program managers who conduct fractional ownership operations under part 91K.

(2) Operations Specifications (OpSpecs). Issued to certificate holders for part 121, 125, 129, 133, 135, 137, 145, or 147.

(3) Letters of Authorization (LOA). Issued to part 91 operators or part 125 operators conducting operations in accordance with a Letter of Deviation Authority (LODA) (identifiable in WebOPSS as "125M").

(4) Training Specifications (TSpecs). Issued to part 61 (flight and ground training providers), part 141 (pilot schools), or part 142 (training centers).

k. Password. An identification code or device required to access stored material, intended to prevent information from being viewed, edited, or printed by unauthorized persons.

l. Private Key. A key pair used to create a digital signature.

m. Public Key. A key pair used to verify a digital signature.

n. Signature. A mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation, and to authenticate a record entry. A signature should be traceable to the individual making the entry, and it should be handwritten or part of an electronic signature system.

1-8. APPROVAL, ACCEPTANCE, AND AUTHORIZATION. There are many 14 CFR part regulations that address electronic signatures, records/recordkeeping, and manuals. There are varying requirements between the many 14 CFR parts for approval, acceptance, and authorization.

a. FAA Approval Required. FAA approval is required to use the following electronic manual and recordkeeping systems:

(1) Electronic MEL. Part 91K, § 91.1115(a)(2); part 121, § 121.628(a)(2); part 125, § 125.201(a)(2); and part 135, § 135.179(a)(2) certificate holders who conduct operations under parts 91K, 121, 125, or 135 must provide flightcrews with direct access to the MEL through printed or other means approved by the Administrator.

(2) Part 121 Crewmember and Dispatcher Records. Section 121.683(c) allows a certificate holder to use a computerized recordkeeping system, approved by the Administrator, to maintain crewmember and dispatcher records required by part 121.

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

b. FAA Acceptance Required. With the exception of the items that require FAA approval (see subparagraph 1-8a above), FAA acceptance is required for certificate holders to use electronic signatures, electronic recordkeeping systems, and electronic manual systems to satisfy the requirements of parts 91K, 121, 125, 133, 135, and 145. FAA acceptance is also required for certificate holders who use electronic records, and the electronic signatures associated with those records, to satisfy the requirements of parts 141, 142, and 147.

c. OpSpec Authorization Required. The FAA will authorize the use of electronic signatures, electronic recordkeeping systems, and electronic manual systems via OpSpec A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems. The A025 template name varies by regulatory part. OpSpec authorization is required for parts 91K, 121, 125, 133, 135, 141, 142, 145, and 147. FAA guidance on the issuance of A025 can be found in FAA Order 8900.1, Flight Standards Information Management System (FSIMS), Volume 3, Chapter 18, Section 3, Part A Operations Specifications—General.

d. The FAA Will Use OpSpec A025 as the Method to Convey Approval, Acceptance, and Authorization. The FAA will use OpSpec A025 as the method to convey FAA approval or acceptance for those items that require specific FAA approval or acceptance to be maintained, accessed, or distributed electronically. The signature on the OpSpec by the FAA principal inspector (PI) or other aviation safety inspector (ASI) with OpSpec signature authority indicates the FAA's approval or acceptance of the item (depending on the requirement). When the FAA issues A025 in WebOPSS, the certificate holder is authorized to use the electronic items listed, as of the effective date of the active OpSpec. This date also signifies the effective date of FAA approval or acceptance.

e. There is No Requirement for Formal Approval, Acceptance, or Authorization for Part 61, 63, 65, 91 (Excluding 91K), 137, or 183. The use of an electronic signature, electronic recordkeeping system, or electronic manual system under part 61, 63, 65, 91 (excluding 91K), 137, or 183 does not require formal FAA approval, acceptance, or authorization. OpSpec (including an MSpec/TSpec/LOA) A025 does not apply to operations under these parts. The FAA recommends that all certificate holders adopt the standards for electronic signatures, records, and manuals as set forth in the AC, 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 standards set forth in this AC, the FAA may question its validity. If the FAA determines that an electronic signature, record, or manual does not meet the standards or is otherwise unacceptable, the FAA office with oversight responsibility will notify the certificate holder in writing. Upon receiving notification, it is incumbent upon the certificate holder to make the appropriate corrections.

CHAPTER 2. ELECTRONIC SIGNATURES

2-1. ELECTRONIC SIGNATURE. The U.S. Electronic Signatures in Global and National Commerce Act (Public Law (PL) 106-229 (also known as E-Sign)) defines an electronic signature as 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."

> **NOTE: Throughout this AC, the term "electronic signature" refers to either electronic signatures or digital signatures. The specific electronic signature used depends on the end user's preference and the system application.**

a. General. The electronic signature's purpose is identical to that of a handwritten signature or any other form of signature currently accepted or approved by the FAA; therefore, electronic signatures must possess those qualities and attributes that guarantee a handwritten signature's authenticity.

> **NOTE: Electronic signatures should only be used to satisfy requirements relating to this AC. They may not be considered acceptable in other areas covered by 14 CFR having more specific applicability (e.g., legal depositions).**

b. Types of Electronic Signatures. Electronic signatures may appear in various formats. No matter the format, they must meet the legal requirements of electronic signing that appear in subparagraph 2-1c. Examples of electronic signature formats include, but are not limited to:

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

c. Electronic Signature Standards. Electronic signatures should meet the following criteria to be considered legally binding.

(1) A person (the signer) must use an acceptable electronic form of signature.

(2) The signature must be unique to the signatory.

(3) There must be a means to identify and authenticate a particular person as the signer.

(4) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record to indicate a person's approval or affirmation of the information contained in the electronic record.

(5) The electronic form of signature must be attached to or associated with the electronic record being signed.

(6) The signature must be permanent and the information to which it is attached must be unalterable without a new signature.

(7) There must be a means to preserve the integrity of the signed record.

(8) 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 (non-repudiation).

d. 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.

(1) 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 plain text 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.

(a) 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 smart cards, digital tokens, access badges, or a user ID.

(b) 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. A private key must be under the sole control of the person using it. The signatory must keep the private key secret and stored in a protected environment.

(c) 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.

(2) 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.

2-2. ELECTRONIC SIGNATURE PROCESS. A certificate holder's electronic signature process should describe, contain, or address the following:

a. Uniqueness. An electronic signature is only valid if it is unique to the individual signatory. It should identify a specific individual and be difficult to duplicate.

b. Control. A valid electronic signature must be under the sole control of the signatory and require the signatory to use a unique user name and password to access the system and affix the signature.

c. Notification. The system should notify the signatory that the signature has been affixed.

d. Intent to Sign. The signatory should be prompted before their signature is affixed. The electronic signature block should contain a word or statement of intent that definitively conveys the signatory's intent to affix his or her signature. Examples of statements that do this include, but are not limited to:

- "Signed by,"
- "Certified by,"
- "Instructor's signature/certification,"
- "Signature,"
- "Authorized by,"
- "Signatory,"
- "Authentication,"
- "Acknowledged by,"
- "Acknowledgement," and/or
- "Affirmed by."

e. Deliberate. An individual using an electronic signature should take deliberate and recognizable action to affix their signature. Acceptable deliberate actions for creating an electronic signature include, but are not limited to, the following:

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

f. Signature Association. A signature must be attached to, or logically associated with, the record being signed; otherwise, it is not legally significant. There are two aspects to this issue:

(1) It must be clear to the signatory exactly what it is that they are signing. In an electronic environment, the signer must have an opportunity to review the record before signing it, and to clearly understand the parameters of the record they are signing. It is also critical that the signing process be established in a manner to ensure that the signatory's electronic signature is applied only to what they can review.

(2) The electronic form of signature applied by the signer must be linked to the record being signed. Satisfying this requirement requires storing the data constituting the electronic form of signature and doing so in a way that permanently associates it with the electronic record that was signed.

g. Retrievable and Traceable. The user should be able to identify and retrieve the documents to which his or her electronic signature has been applied. An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

h. Undeniable. A valid electronic signature is one that cannot be denied (repudiated) by the signer. An electronic signature process must contain procedures and controls designed to ensure the authenticity of the signature and that the signer cannot deny having affixed the signature to a specific record, document, or body of data.

i. Security Protocols and Prevention of Unauthorized Access and Modification. An 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 must contain restrictions and procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment.

j. Permanent and Unalterable. 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.

k. Identification and Authentication. Electronic signature software must have authentication capabilities that can identify a signature as belonging only to a particular signatory. An individual using an electronic signature should be required to use a method of authentication that positively identifies the individual within the electronic signature system.

l. 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.

m. Archivable. Since no paper document with an ink signature exists, a means of safely archiving electronically signed documents should be part of any electronic signature computer software.

n. 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.

o. Policies and Procedures. When constructing an electronic signature process, the certificate holder's manual should include the following elements:

(1) Procedures. Procedures should address how the applicable regulatory requirements for their program are met. These procedures should be available to all users of the system.

(2) Description of Electronic Signature Process. A description of the electronic signature process must be included in the certificate holder's manual. 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). 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 in an official document maintained by the certificate holder.

(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) Identification of Persons Authorized to Use Electronic Signatures. Certificate holders must have a system for identifying who is authorized to use the electronic signature process, for what purposes, and which records.

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

(6) Hardware and Software Capabilities. Description(s) of the electronic signature hardware to be used and software capabilities for applications of electronic signatures in the certificate holder's system(s).

(7) Auditing Process. Electronic signature policies and procedures should include an auditing process to 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. 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 AC applies, revisions to the electronic signature process must be included in the manual or official document containing the electronic signature process description.

(9) Data Backup and Retention. Policy and procedures should address how data backup and retention of data will be accomplished.

(10) Procedures for Computer System Outages and/or Disaster Recovery. Policy and procedures should address computer system outages (failure of hardware, software, application, network, etc.) or disaster recovery.

(11) 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. Procedures should describe how users are notified of changes to the electronic signature process.

2-3. ELECTRONIC SIGNATURE AUTHORIZATION.

a. Application Submission. Certificate holders should submit their application to use an electronic signature process to their certificate-holding district office (CHDO). The application medium (paper or electronic file) must be acceptable to both the applicant and the FAA. The FAA will review the application package according to the General Process for Approval or Acceptance of Air Operator Applications contained in FAA Order 8900.1, Flight Standards Information Management System (FSIMS), Volume 3, Chapter 1, The General Process for Approval or Acceptance of Air Operator Applications. The FAA will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The FAA may also notify the certificate holder in writing of any application deficiencies. Before the CHDO accepts the application package, the certificate holder will be required to correct all of the deficiencies. A certificate holder's application package for authorization to use electronic signatures must include the following:

(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 process application.

(2) A Description of the Proposed Electronic Signature Process. The electronic signature process description must address all of the requirements contained in paragraphs 2-1 and 2-2 of this AC.

(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. The FAA will require a certificate holder to demonstrate the electronic signature process. The items requiring demonstration will typically include at least 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 are prevented without a new signature.

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

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

c. Successful Completion of Application Process for Acceptance and Authorization. When a certificate holder successfully completes the application and demonstration process, the FAA will accept the electronic signature process and authorize its use by signing and issuing Operations Specification (OpSpec) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the electronic signature process, the CHDO will reject the application and provide an explanation to the certificate holder in writing.

CHAPTER 3. ELECTRONIC RECORDKEEPING

3-1. 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 should contain enough information to clearly depict the event that took place. It is the certificate holder's responsibility to address all 14 CFR requirements for their recordkeeping system(s) applicable to their operation(s).

3-2. FAA STANDARDS FOR ELECTRONIC RECORDS. To be considered complete and valid, an electronic record should contain at least the following information:

- The type of event that took place (e.g., training, maintenance performed, signing of a release, conduct of a flight, etc.);
- 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.;
- When the event took place (e.g., the date and time (where appropriate));
- Where the event took place (e.g., the station, training facility, maintenance facility, etc.);
- Who was involved in the event (e.g., crewmember, dispatcher, instructor, mechanic, etc.);
- Aircraft type and registration number for pilot logbook records (when required by regulation);
- Certification, verification, or authentication of the event, such as a signature, where required by regulation; and
- Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (M/M) for maintenance records, such as life-limited parts and time-in-service records.

3-3. ELECTRONIC RECORDKEEPING SYSTEM. Electronic recordkeeping system(s) should include the following elements:

a. Security.

(1) The system should protect confidential information.

(2) The system must ensure that the information in an electronic record is not altered in an unauthorized way.

(3) The system must provide for secure access and contain safeguards against unauthorized access.

b. Procedures. Electronic recordkeeping system procedures must be incorporated into the certificate holder's manual system. For those certificate holders who are not required to have manuals (e.g., 14 CFR part 135 single pilot and 14 CFR part 141), a standalone electronic recordkeeping system procedures document is an acceptable alternative, provided it is an official document maintained by the certificate holder. Procedures should include at least the following:

(1) 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 Operations Specification (OpSpec) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems. 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.

(2) Quality Control (QC). The system should have procedures for auditing the computer system periodically to ensure the quality, integrity, and accuracy of the system. If workstations are server-based and contain no inherent attributes that enable or disable access, there is no need for each workstation to be audited. (A record of the audit should be completed and retained on file as part of the certificate holder's record retention requirements. This audit may be a computer program that automatically audits itself.)

(3) 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 backup system 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.

(4) Record Transfer. Procedures should ensure that records transferred with an aircraft (either electronic or on paper) meet regulatory requirements (i.e., 14 CFR part 43, § 43.10; part 91, § 91.419; part 121, § 121.380a; and part 135, § 135.441).

(5) Persons with Authorized Access. The system procedures should contain guidelines for authorized representatives of the certificate holder to use electronic recordkeeping and to have access to the appropriate records (each representative with authorization to make entries shall be issued a unique individual access code and password in order to validate the entry). In particular, procedures should specifically address instructor, evaluator, and supervisor access to the system.

(6) Electronic Authentication, Signature, Validation, or Endorsement. Most records required by 14 CFR require some kind of validation, such as a signature, certification, endorsement, or authentication. This validation must be a permanent part of any electronic record. Any electronic form of validation must meet the legal requirements of electronic signing as outlined in this AC. The certificate holder must also have authorization to use an electronic signature in OpSpec A025.

(7) Training and User Instructions. Each electronic recordkeeping system should contain training and user instructions for the 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.

(8) Transferring Data. 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.

(9) Continuity of Data Between Legacy and Electronic Systems. The system should have a method of ensuring continuity of data during transition from a legacy (hardcopy) system to an electronic system.

(10) Continuity of Records for Maintenance Providers. Procedures should ensure continuity with maintenance providers. Certificate holders must ensure there is continuity between their program(s) and their maintenance provider's programs. This is necessary to ensure the quality and integrity of each record that is maintained via the electronic recordkeeping system.

c. 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 recordkeeping system 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 recordkeeping system, as well as those who are responsible for entering data into the system.

d. Description of Electronic Recordkeeping System(s). There may be more than one system required to maintain various kinds of records. Each electronic recordkeeping system used by the certificate holder must be described in its manual. The manual containing the description will be included in the OpSpec A025 authorization for parts 91K, 121, 125, and 135. For those certificate holders who are not required to have a manual, a standalone electronic recordkeeping system procedures document is an acceptable alternative, provided it is an official document maintained by the certificate holder. Each electronic recordkeeping system description should address the information and elements contained in paragraphs 3-1, 3-2, and 3-3 of this AC, as well as the following:

(1) Description of electronic recordkeeping system(s) to include system facilities, hardware, and software.

(2) Identification of records that will be maintained in the electronic system(s).

(3) Identification of which electronic records on which the certificate holder will use an authorized electronic signature process.

e. Changes to the Electronic Recordkeeping System. 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 AC applies, changes to the electronic recordkeeping system must be included in the manual or official document containing the electronic recordkeeping system description.

f. Audit Procedures. The certificate holder must have auditing procedures that ensure the quality and integrity of each record maintained in the system and that all of the requirements of the electronic recordkeeping system continue to be met. 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.

3-4. ELECTRONIC RECORDKEEPING AUTHORIZATION.

a. Application. Certificate holders should submit their application for an electronic recordkeeping process to their certificate-holding district office (CHDO). The application medium (paper or electronic file) must be acceptable to both the applicant and the FAA. The FAA will review the application package according to the General Process for Approval or Acceptance of Air Operator Applications contained in FAA Order 8900.1, Flight Standards Information Management System (FSIMS), Volume 3, Chapter 1, The General Process for Approval or Acceptance of Air Operator Applications. The FAA will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The FAA may also notify the certificate holder in writing of any application deficiencies. Before the CHDO accepts the application package, the certificate holder will be required to correct all of the deficiencies A certificate holder's application package for authorization to use an electronic record keeping system must include the following:

(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 Point of Contact (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 paragraphs 3-1, 3-2, and 3-3 of the AC, 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 electronic record category.

b. Demonstration of the System. The FAA will require a certificate holder to demonstrate the electronic record keeping system. The items requiring demonstration will typically include at least 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. Successful Completion of Application Process for Approval or Acceptance and Authorization. When the certificate holder successfully completes the application and demonstration process, the FAA will accept or approve (depending on the regulatory requirement) the electronic recordkeeping system and authorize its use by signing and issuing OpSpec A025.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the electronic recordkeeping process, the CHDO will reject the application and provide an explanation to the certificate holder in writing.

CHAPTER 4. ELECTRONIC MANUAL SYSTEMS

4-1. ELECTRONIC MANUALS. 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 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. An electronic manual should contain 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;
- 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 (M/M) (when applicable for minimum equipment list (MEL) and maintenance purposes); and
- The person with the authority and responsibility for manual content.

4-2. ELECTRONIC MANUAL SYSTEM. An electronic system for delivering manual content must comply with regulatory requirements for currency, availability, and distribution to the appropriate personnel. A certificate holder's electronic manual system must address any 14 CFR part requirements for "must" or "should" that apply to their operation(s) into their electronic manual system. An electronic manual system should describe/address:

a. Currency. Each certificate holder's electronic manual system method of keeping each manual current.

b. Access, Availability, and Distribution. Each electronic manual system should provide distribution and/or access to manual(s) by the appropriate personnel, in a form and method acceptable to the Administrator.

c. MEL Direct Access Requirement. As required by part 91, § 91.1115(a)(2); part 121, § 121.628(a)(2); part 125, § 125.201(a)(2); and part 135, § 135.179(a)(2) certificate holders who conduct operations under part 91K, 121, 125, or 135 must provide flightcrews with direct access to the MEL through printed or other means approved by the Administrator. An Electronic Flight Bag (EFB) is an example of other means that may be approved by the FAA.

d. FAA/National Transportation Safety Board (NTSB) Access. The FAA encourages certificate holders to provide access to the electronic manual system to the appropriate FAA representatives assigned to the certificate holder. When providing such access, a certificate holder should provide the FAA's representatives with instructions on how to access the system. Certificate holders 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, it should be provided in the desired format of the requesting agency whenever possible.

e. Responsible Personnel. The system description should include the certificate holder's personnel who have 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.

g. Storage and Retrieval. The computer hardware and software system must store and retrieve the manual's content under conditions of normal operation and use. The system must not permit unauthorized modification of the data it contains.

h. Functionality. 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.

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. The revision system should make changes under the current revision readily apparent. An example of this would be change bars. An 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 the 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 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 hardware or software failure. The backup method may be a separate electronic system; a backup server to the authorized system; the use of 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 4-2m above.

o. 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 principal inspector (PI) will reference when accepting the electronic manual system and authorizing its use in Operations Specification (OpSpec) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems. 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 the 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 kids of manuals, instead of listing each manual, provided all of the particular kinds of manuals are maintained and distributed via the electronic manual system. For example, list "All Ground Operations Manuals," "All Maintenance Manuals," or "All Training Program Manuals."

p. Description of the Electronic Manual—Parts 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.

q. Electronic Manual System Changes. Policy 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.

r. User Instructions and Training. Each certificate holder must provide instructions and training 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.

4-3. ELECTRONIC MANUAL AUTHORIZATION.

a. Application. Certificate holders should submit their application for an electronic manual system to their certificate-holding district office (CHDO). The application medium (paper or electronic file) must be acceptable to both the applicant and the FAA. The FAA will review the application package according to the General Process for Approval or Acceptance of Air Operator Applications contained in FAA Order 8900.1, Flight Standards Information Management System (FSIMS), Volume 3, Chapter 1. The FAA will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The FAA may also notify the certificate holder in writing of any application deficiencies. Before the CHDO accepts the application package, the certificate holder will be required to correct all of the deficiencies. A certificate holder's application package for authorization to use an electronic manual or manual system must include the following:

(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 Point of Contact (POC). The letter must include the certificate holder's primary POC for the electronic manual system application process.

(2) Master Manual 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 4-2o of this AC.

(3) A Description of the Proposed Electronic Manual—Part 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 paragraph 4-2p of this AC.

(4) Manuals Included in the System. The application must state specifically which manuals the certificate holder intends to maintain and distribute electronically:

- Flight Operations Manuals (FOM) by title;
- Ground operations manuals by title;
- Maintenance manuals by title;
- Training program manuals by title;
- Electronic MELs;
- General policy manuals by title; and
- 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. The FAA will require a certificate holder to demonstrate the electronic manual system. The items requiring demonstration will typically include at least 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. Successful Completion of Application for Approval or Acceptance and Authorization. When a certificate holder successfully completes the approval (applicable only to electronic access to an MEL) or acceptance process, the FAA will authorize the electronic manual system by signing and issuing OpSpec A025.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the manual system process, the CHDO will reject the application and provide an explanation to the certificate holder in writing.

CHAPTER 5. VOLUNTARY DISCONTINUANCE BY CERTIFICATE HOLDER

5-1. VOLUNTARY DISCONTINUANCE. If a certificate holder elects to discontinue using electronic signatures, an electronic recordkeeping system, or an electronic manual system, it must inform the appropriate principal inspector (PI) or aviation safety inspector (ASI) by letter. Once informed, the CHDO will amend the certificate holder's Operations Specification (OpSpec) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems, to remove the authorization voluntarily discontinued. Certificate holders that voluntarily discontinue the use of electronic signatures, an electronic recordkeeping system, and/or an electronic manual system must include the following information in their discontinuance letter.

a. Discontinue Electronic Signatures.

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

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

(3) 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.

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

b. Discontinue Electronic Recordkeeping System.

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

(2) 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 match the electronic content, including having the required signatures.

c. Discontinue Electronic Manual System.

(1) The letter from the certificate holder must include the projected date the certificate holder intends to discontinue using the system and provide hardcopy manuals, if required by appropriate 14 CFR parts.

(2) 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.

CHAPTER 6. ADMINISTRATIVE

6-1. QUESTIONS ABOUT THIS AC. If you have questions about the material in this AC or would like to provide feedback, you may contact the Aircraft Maintenance Division (AFS-300) at 5th Floor, 950 L'Enfant Plaza, SW., Washington, DC 20024; or by phone at 202-267-1675. For your convenience, the Advisory Circular Feedback Form is the last page of this AC.

6-2. OTHER RELATED REGULATIONS, GUIDANCE, AND READING MATERIAL.

a. Regulatory References (current editions):

- Electronic Signatures in Global and National Commerce Act (E-Sign) (Public Law (PL) 106-229, Title I).
- Government Paperwork Elimination Act (GPEA) (PL 105-277, Title XVII).
- Paperwork Reduction Act (PL 104-13).
- Title 14 CFR Parts 43, 61, 65, 91, 119, 121, 125, 129, 133, 135, 137, 141, 142, 145, and 147.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources.

b. FAA Order 8900.1, Flight Standards Information Management System (FSIMS).

c. Part 121 Dispatch and Flight Release Requirements—Electronic Signatures, Amendments and Disposition. Information regarding electronic signatures on a dispatch or flight release; electronic amendments to a dispatch or flight release; and/or electronic recordkeeping of a dispatch or flight release is contained in Order 8900.1, Volume 3, Chapter 25, Section 1, General Topics.

d. Part 121 En Route Communication Records. Information on the electronic retention of en route communication records in accordance with part 121, § 121.711 is contained in Order 8900.1, Volume 3, Chapter 25, Section 1.

e. Part 121 and 135 Recordkeeping Systems Acceptance or Approval Process. Information and guidance to be used by principal inspectors (PI) when accepting or approving certificate holder recordkeeping systems is contained in Order 8900.1, Volume 3, Chapter 31, Section 2, Requirements for Approval, Acceptance, and Authorization.

f. Part 121 and 135 Crewmember and Aircraft Dispatcher Records. Order 8900.1, Volume 3, Chapter 31, Section 3, Crewmember and Aircraft Dispatcher Records, contains detailed information regarding crewmember and aircraft dispatcher records in accordance with the requirements of parts 121 and 135, as applicable.

g. Part 121 and Part 135, § 135.411(a)(2) Maintenance Records. Order 8900.1, Volume 3, Chapter 31, Section 5, Safety Assurance System: Evaluate a Part 121/135 (10 or More) Certificate Holder/Applicant Maintenance Recordkeeping System, contains detailed information regarding the evaluation of an air carrier's maintenance recordkeeping system.

h. Part 91K Non-CAMP Program Manager's, Part 125, § 125.247 Certificate Holder's, and § 135.411(a)(1) Maintenance Records. Order 8900.1, Volume 3, Chapter 31, Section 6, Safety Assurance System: Evaluate a Part 91K Non-CAMP Program Manager's, § 125.247 Operator's, and § 135.411(a)(1) Certificate Holder's Maintenance Records, contains information for Airworthiness inspectors on how to evaluate part 91K non-CAMP and part 135 maintenance records.

i. Part 145. Order 8900.1, Volume 6, Chapter 9, Section 6, Safety Assurance System: Inspect a Repair Station's Record System, contains detailed information on repair station electronic signatures and electronic recordkeeping.

j. Operations Specification (OpSpec) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems. Information on how to issue OpSpec A025 is contained in Order 8900.1, Volume 3, Chapter 18, Section 3, Part A Operations Specifications—General, OpSpec/management specification (MSpec) A025.

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

l. Related ACs (current editions):

- 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.

m. Other Reading Material. OMB Memorandum 00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act.

6-3. OBTAINING REFERENCE MATERIAL (current editions):

- You can find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.
- Certificate holders can find this AC and Order 8900.1 at http://fsims.faa.gov.

APPENDIX 1. SAMPLE LETTER OF INTENT

[Requester Letterhead]

To: [FAA certificate-holding district office (CHDO)/Flight Standards District Office (FSDO) with jurisdiction over the requester's operations]

From: [Requester]

Date: [Date]

Subject: Use of Electronic System – (Signatures/Recordkeeping/Manuals)

This letter is to inform you that [requester] intends to use an electronic (signatures and/or recordkeeping and/or manual) system for [describe what the system will be used for]. This system has been established using the guidelines outlined in FAA Advisory Circular (AC) 120-78 (as amended).

NOTE: Certificate holders should use this AC to identify the various requirements for the letter of intent contents.

Company facilities, equipment, and personnel are available for your review at [address] on [date]. Please contact [name] at [telephone] to arrange a visit to review the system and to discuss any FAA concerns.

Sincerely,

[Requester]

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by contacting the Flight Standards Directives Management Officer at 9-AWA-AFS-140-Directives@faa.gov.

Subject: AC 120-78A, Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals

Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

_____

_____

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

_____

_____

☐ Other comments:

_____

_____

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____