VOLUME 3 GENERAL TECHNICAL ADMINISTRATION

CHAPTER 31 ELECTRONIC SIGNATURES, ELECTRONIC RECORDKEEPING SYSTEMS, AND ELECTRONIC MANUAL SYSTEMS

Section 1 General – Definitions and Terminology

3-2981 GENERAL. This chapter contains information regarding Federal Aviation Administration (FAA) approval or acceptance of a certificate holder's electronic manuals, electronic recordkeeping systems, and electronic signatures. This section contains a general overview of the characteristics and requirements of electronic manuals, records, and signatures. This section also contains terminology and definitions used throughout this chapter. This section is related to Safety Assurance System (SAS) subsystems 3.3, Flight Planning and Monitoring; 4.2, Maintenance Planning and Monitoring; and 4.3, Maintenance Operations.

A. Scope. This section applies to principal inspectors (PI) and aviation safety inspectors (ASI) 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 signature, recordkeeping, and manual requirements contained in Title 14 of the Code of Federal Regulations (14 CFR).

B. Applicability. The definitions, requirements, and guidelines contained in this section apply anywhere 14 CFR requires a signature, record, or manual.

3-2982 TERMINOLOGY. The following terminology is used throughout this chapter:

A. Certificate-Holding District Office (CHDO). Unless otherwise noted, the acronym "CHDO" will be used throughout this chapter to describe a Flight Standards (AFS) field office with oversight responsibility. The acronym "CHDO" applies to a certificate management office (CMO), a Flight Standards District Office (FSDO), an International Field Office (IFO), or an International Field Unit (IFU).

B. Operations Specification (OpSpec). Unless otherwise noted, the term "OpSpec" will be used throughout this chapter to describe authorizing documents located in the Web-based Operations Safety System (WebOPSS). An authorizing document in WebOPSS is either a management specification (MSpec) (14 CFR part 91K); OpSpec (14 CFR parts 121, 125, 129, 133, 135, 145, and 147); letter of authorization (LOA) (14 CFR parts 91 and 137 certificate holders and part 125 Letter of Deviation Authority (LODA) holders); or training specification (TSpec) (14 CFR part 61 flight and ground instructors, 14 CFR part 141 pilot schools, and 14 CFR part 142 training center certificate holders). This section uses the singular term "OpSpec" for simplicity.

C. Certificate Holder. Unless otherwise noted, the term "certificate holder" is used in this chapter to identify air carries, program managers, operators, air agencies, and any other FAA-regulated entities under 14 CFR to which electronic signatures, records, and manuals apply.

3-2983 DEFINITIONS. The following definitions are used throughout this chapter:

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, a badge swipe, or a stamp.

B. Authorization. Official permission.

C. Calendar-Month. The first day through the last day of a particular month.

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

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

F. Data Entry. The process by which data or information is entered into a computer memory or storage medium. Sources include manually written records, real-time information, and computer-generated data.

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

H. Database Management System (DBMS). A computer software program capable of maintaining stored information in an ordered format, manipulating that data by mathematical methods, and performing data processing functions, such as retrieval of data.

I. Digital Signature. Cryptographically generated data that identifies a document's signatory (signer) and certifies that the document has not been altered. This technology is based on public/private key cryptography, digital signature technology used in secure messaging, Public Key Infrastructure (PKI), virtual private network (VPN), Web standards for secure transactions, and electronic digital signatures.

J. Electronic Manuals. Consists of operational and/or maintenance manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, Internet/Intranet-based, or in other various forms of electronic media. Electronic manuals may consist of accepted or approved data and/or reference data used in aircraft maintenance or operations.

NOTE: For the purpose of this chapter, electronic manuals do not include those manuals created under a manufacturing authority (e.g., type certificate (TC), Supplemental Type Certificate (STC), and Parts Manufacturer Approval (PMA)), such as Original Equipment Manufacturer (OEM) flight manuals, OEM maintenance manuals, and OEM overhaul manuals. The FAA's Aircraft Certification Service (AIR) establishes the requirements and standards for these

kinds of manuals. The policies and standards in this chapter are set forth by AFS and are intended for those entities regulated by AFS.

K. Electronic Record. A record (including contracts and OpSpecs) created, generated, sent, communicated, received, or stored by electronic means.

L. Electronic Recordkeeping System. A system of record processing in which records are entered, electronically signed, stored, and retrieved electronically by a computer system rather than in the traditional "hardcopy" or paper form.

M. Electronic Signature. The electronic equivalent of a handwritten signature. It is an electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by an individual with the intent to sign. It electronically identifies and authenticates an individual and combines cryptographic functions of digital signatures with the image of an individual's handwritten signature or some other visible mark considered acceptable in a traditional signing process. It authenticates data, provides permanent, secure user authentication, and is considered to be the legally binding equivalent of the individual's handwritten signature.

N. Electronic Technology. Relating to or having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

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

P. Private Key. The key of a key pair used to create a digital signature.

Q. Proprietary Information. Information that is the private property of the certificate holder.

R. Public Key. The key of a key pair used to verify a digital signature.

S. Real-Time Record. Information that is entered into a computer-based recordkeeping system immediately following the completion of an event or fulfillment of a condition without first relying on the manual recording of the information on a data entry form.

T. Record. Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

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

V. System Security. Policies, procedures, and system structures designed to prevent users from gaining unauthorized access.

W. User Identification. A series of alphanumeric characters assigned to an individual for the purpose of gaining access to a computer system and accounting for time usage.

RESERVED. Paragraphs 3-2984 through 3-2998.