(1) *Alternative Methods of Compliance (AMOCs):* The Manager, International Branch, ANM–116, Transport Airplane Directorate, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or local Flight Standards District Office, as appropriate. If sending information directly to the International Branch, send it to ATTN: Tom Rodriguez, Aerospace Engineer, International Branch, ANM–116, Transport Airplane Directorate, FAA 1601 Lind Avenue SW., Renton, WA 98057–3356; telephone (425) 227–1137; fax (425) 227–1149. Information may be emailed to: *9-ANM-116-AMOC-REQUESTS@faa.gov.* Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the local flight standards district office/certificate holding district office. The AMOC approval letter must specifically reference this AD.

(2) *Airworthy Product:* For any requirement in this AD to obtain corrective actions from a manufacturer or other source, use these actions if they are FAA-approved. Corrective actions are considered FAA-approved if they are approved by the State of Design Authority (or their delegated agent). You are required to assure the product is airworthy before it is returned to service.

(i) Related Information

Refer to MCAI European Aviation Safety Agency Airworthiness Directive 2011–0183, dated September 23, 2011; and Fokker Service Bulletin SBF100–24–044, dated July 14, 2011, including Fokker Manual Change Notification—Maintenance Documentation MCNM–F100–148, dated July 14, 2011; for related information.

(j) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) Fokker Service Bulletin SBF100–24–044, dated July 14, 2011, including Fokker Manual Change Notification—Maintenance Documentation MCNM–F100–148, dated July 14, 2011.

(ii) Reserved.

(3) For service information identified in this AD, contact Fokker Services B.V., Technical Services Dept., P.O. Box 231, 2150 AE Nieuw-Vennep, the Netherlands; telephone +31 (0)252–627–350; fax +31 (0)252–627–211; email *technicalservices.fokkerservices@stork.com;* Internet *http://www.myfokkerfleet.com.*

(4) You may review copies of the service information at the FAA, Transport Airplane Directorate, 1601 Lind Avenue SW., Renton, WA. For information on the availability of this material at the FAA, call 425–227–1221.

(5) You may view this service information that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030, or go to: *http://www.archives.gov/federal-register/cfr/ibr-locations.html.*

Issued in Renton, Washington, on September 11, 2012.

Ali Bahrami,

Manager, Transport Airplane Directorate, Aircraft Certification Service.

[FR Doc. 2012–23055 Filed 9–21–12; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

21 CFR Part 1300

Definitions Relating to Electronic Orders and Prescriptions for Controlled Substances

CFR Correction

In Title 21 of the Code of Federal Regulations, Part 1300 to End, revised as of April 1, 2012, on page 14, § 1300.03 is reinstated to read as follows:

§ 1300.03 Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.

For the purposes of this chapter, the following terms shall have the meanings specified:

Application service provider means an entity that sells electronic prescription or pharmacy applications as a hosted service, where the entity controls access to the application and maintains the software and records on its servers.

Audit trail means a record showing who has accessed an information technology application and what operations the user performed during a given period.

Authentication means verifying the identity of the user as a prerequisite to allowing access to the information application.

Authentication protocol means a well specified message exchange process that verifies possession of a token to remotely authenticate a person to an application.

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable.

Biometric subsystem means the hardware and software used to capture, store, and compare biometric data. The biometric subsystem may be part of a larger application. The biometric subsystem is an automated system capable of:

(1) Capturing a biometric sample from an end user.

(2) Extracting and processing the biometric data from that sample.

(3) Storing the extracted information in a database.

(4) Comparing the biometric data with data contained in one or more reference databases.

(5) Determining how well the stored data matches the newly captured data and indicating whether an identification or verification of identity has been achieved.

Cache means to download and store information on a local server or hard drive.

Certificate policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate revocation list (CRL) means a list of revoked, but unexpired certificates issued by a certification authority.

Certification authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

Certified information systems auditor (CISA) means an individual who has been certified by the Information Systems Audit and Control Association as qualified to audit information systems and who performs compliance audits as a regular ongoing business activity.

Credential means an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Credential service provider (CSP) means a trusted entity that issues or registers tokens and issues electronic credentials to individuals. The CSP may be an independent third party or may issue credentials for its own use.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum—

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the certification authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Digitally sign means to affix a digital signature to a data file.

Electronic prescription means a prescription that is generated on an electronic application and transmitted as an electronic data file.

Electronic prescription application provider means an entity that develops or markets electronic prescription software either as a stand-alone application or as a module in an electronic health record application.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

False match rate means the rate at which an impostor's biometric is falsely accepted as being that of an authorized user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false accept (or acceptance) rate.

False non-match rate means the rate at which a genuine user's biometric is falsely rejected when the user's biometric data fail to match the enrolled data for the user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false reject (or rejection) rate, except that it does not include the rate at which a biometric system fails to acquire a biometric sample from a genuine user.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in § 1311.08 of this chapter, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140–2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Security Requirements for Cryptographic Modules,'' a Federal standard for security requirements for cryptographic modules.

FIPS 180–2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Secure Hash Standard,'' a Federal secure hash standard.

FIPS 180–3, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Secure Hash Standard (SHS),'' a Federal secure hash standard.

FIPS 186–2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Digital Signature Standard,'' a Federal standard for applications used to generate and rely upon digital signatures.

FIPS 186–3, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Digital Signature Standard (DSS),'' a Federal standard for applications used to generate and rely upon digital signatures.

Hard token means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card, USB drive, one-time password device) rather than on a general purpose computer.

Identity proofing means the process by which a credential service provider or certification authority validates sufficient information to uniquely identify a person.

Installed electronic prescription application means software that is used to create electronic prescriptions and that is installed on a practitioner's computers and servers, where access and records are controlled by the practitioner.

Installed pharmacy application means software that is used to process prescription information and that is installed on a pharmacy's computers or servers and is controlled by the pharmacy.

Intermediary means any technology system that receives and transmits an electronic prescription between the practitioner and pharmacy.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

NIST SP 800–63–1, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Electronic Authentication Guideline,'' a Federal standard for electronic authentication.

NIST SP 800–76–1, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ''Biometric Data Specification for Personal Identity Verification,'' a Federal standard for biometric data specifications for personal identity verification.

Operating point means a point chosen on a receiver operating characteristic (ROC) curve for a specific algorithm at which the biometric system is set to function. It is defined by its corresponding coordinates—a false match rate and a false non-match rate. An ROC curve shows graphically the trade-off between the principal two types of errors (false match rate and false non-match rate) of a biometric system by plotting the performance of a specific algorithm on a specific set of data.

Paper prescription means a prescription created on paper or computer generated to be printed or transmitted via facsimile that meets the requirements of part 1306 of this chapter including a manual signature.

Password means a secret, typically a character string (letters, numbers, and other symbols), that a person memorizes and uses to authenticate his identity.

PDA means a Personal Digital Assistant, a handheld computer used to manage contacts, appointments, and tasks.

Pharmacy application provider means an entity that develops or markets software that manages the receipt and processing of electronic prescriptions.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certificate revocation list.

Readily retrievable means that certain records are kept by automatic data processing applications or other electronic or mechanized recordkeeping systems in such a manner that they can be separated out from all other records in a reasonable time and/or records are kept on which certain items are asterisked, redlined, or in some other

manner visually identifiable apart from other items appearing on the records.

SAS 70 Audit means a third-party audit of a technology provider that meets the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 70 criteria.

Signing function means any keystroke or other action used to indicate that the practitioner has authorized for transmission and dispensing a controlled substance prescription. The signing function may occur simultaneously with or after the completion of the two-factor authentication protocol that meets the requirements of part 1311 of this chapter. The signing function may have different names (e.g., approve, sign, transmit), but it serves as the practitioner's final authorization that he intends to issue the prescription for a legitimate medical reason in the normal course of his professional practice.

SysTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of electronic systems.

Third-party audit means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Token means something a person possesses and controls (typically a key or password) used to authenticate the person's identity.

Trusted agent means an entity authorized to act as a representative of a certification authority or credential service provider in confirming practitioner identification during the enrollment process.

Valid prescription means a prescription that is issued for a legitimate medical purpose by an individual practitioner licensed by law to administer and prescribe the drugs concerned and acting in the usual course of the practitioner's professional practice.

WebTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of Web sites.

[75 FR 16304, Mar. 31, 2010]

[FR Doc. 2012–23529 Filed 9–21–12; 8:45 am]

BILLING CODE 1505–01–D

DEPARTMENT OF THE INTERIOR

National Indian Gaming Commission

25 CFR Parts 502 and 559

RIN 3141–AA48

Facility License Notifications and Submissions

AGENCY: National Indian Gaming Commission.

ACTION: Final rule.

SUMMARY: The National Indian Gaming Commission (NIGC or Commission) is amending its facility license regulations. The final rule amends the current regulations: To provide for an expedited review to confirm a tribe's submittal of facility license information; to require notice to the NIGC when a tribe issues, renews, or terminates a facility license; to streamline the submittal of certain information relating to the construction, maintenance, and operation of a gaming facility; and to provide that a tribe need not submit a notification of seasonal or temporary closures of less than 180 days.

DATES: The effective date of these regulations is October 24, 2012.

FOR FURTHER INFORMATION CONTACT: Armando Acosta, National Indian Gaming Commission, 1441 L Street NW., Suite 9100, Washington, DC 20005. Email: *armando_acosta@nigc.gov;* telephone: 202–632–7003.

SUPPLEMENTARY INFORMATION:

I. Background

The Indian Gaming Regulatory Act (IGRA or Act), Public Law 100–497, 25 U.S.C. 2701, *et seq.,* was signed into law on October 17, 1988. The Act established the Commission and set out a comprehensive framework for the regulation of gaming on Indian lands.

The Act provides for tribal gaming on Indian lands within such tribe's jurisdiction. 25 U.S.C. 2710. The Act requires ''a separate license issued by the Indian tribe * * * for each place, facility, or location on Indian lands at which Class II (and Class III) gaming is conducted.'' 25 U.S.C. 2710(b)(1) and (d)(1)(A)(iii). The Act also requires that tribal ordinances provide that ''the construction and maintenance of the gaming facilities, and the operation of that gaming is conducted in a manner which adequately protects the environment and public health and safety.'' 25 U.S.C. 2710(b)(2)(E).

Part 559 of the NIGC's regulations serves three purposes. The first is for the Commission to receive information from tribes regarding the Indian lands status of each gaming facility. The second is for the Commission to obtain information from tribal governments regarding the construction, maintenance, and operation of the gaming facilities. Finally, part 559 serves to inform the Commission of those places, facilities, or locations at which Indian gaming is presently being conducted.

II. Previous Rulemaking Activity

On November 18, 2010, the Commission issued a Notice of Inquiry and Notice of Consultation advising the public that the NIGC was conducting a comprehensive review of its regulations and requesting public comment on which of its regulations were most in need of revision, in what order the Commission should review its regulations, and the process that the Commission should utilize to make revisions. 75 FR 70680, Nov. 18, 2010. On April 4, 2011, after holding eight consultations and reviewing all comments, the Commission published a Notice of Regulatory Review Schedule (NRRS) setting forth a consultation schedule and process for review. 76 FR 18457, April 4, 2011. Part 559 was included in the first regulatory group reviewed pursuant to the NRRS.

The Commission conducted multiple tribal consultations as part of its review of part 559. Tribal consultations were held in every region of the country and attended by tribal leaders or their representatives. In addition to tribal consultations, on June 11, 2011, the Commission requested public comment on a preliminary draft of amendments to part 559. After considering all public comments, the Commission published a Notice of Proposed Rulemaking. 77 FR 4731, Jan. 31, 2012.

III. Review of Public Comments

In response to its Notice of Proposed Rulemaking, published January 31, 2012, the Commission received the following comments:

559.1 What is the scope and purpose of this part?

Comment: Commenters stated generally that the prior versions of the facility license rules are troublesome and that the proposed amendments to the rules alleviate much of that concern.

Response: The Commission agrees.

559.2 When must a tribe notify the chair that it is considering issuing a new facility license?

Comment: A few commenters questioned the need for a 120-day notification period prior to the opening