

§ 1305.26 Lost electronic orders.

(a) If a purchaser determines that an unfilled electronic order has been lost before or after receipt, the purchaser must provide, to the supplier, a signed statement containing the unique tracking number and date of the lost order and stating that the goods covered by the first order were not received through loss of that order.

(b) If the purchaser executes an order to replace the lost order, the purchaser must electronically link an electronic record of the second order and a copy of the statement with the record of the first order and retain them.

(c) If the supplier to whom the order was directed subsequently receives the first order, the supplier must make an electronic record, indicate that it is "Not Accepted," and return it to the purchaser. The purchaser must link the returned order to the record of that order and the statement.

§ 1305.27 Preservation of electronic orders.

(a) A purchaser must, for each order filled, retain the original signed order and all linked records for that order for two years. The purchaser must also retain all copies of each unaccepted or defective order and each linked statement.

(b) A supplier must retain each original order filled and the linked records for two years.

(c) If electronic order records are maintained on a central server, the records must be readily retrievable at the registered location.

§ 1305.28 Canceling and voiding electronic orders.

A supplier may void all or part of an electronic order by notifying the purchaser of the voiding. If the entire order is voided, the supplier must make an electronic copy of the order, indicate on the copy "Void," and return it to the purchaser. The purchaser must retain an electronic copy of the voided order. To partially void an order, the supplier must indicate on the annotated copy that nothing was shipped for each item voided.

§ 1305.29 Reporting to DEA.

A supplier must, for each electronic order filled, forward either a copy of the electronic order or an electronic report of the order in such format as DEA may specify to DEA every other business day. For suppliers who choose to submit a report rather than copies, the report must include the following data fields for each order filled:

- (a) The supplier's name.
- (b) The supplier's complete address.

(c) The supplier's DEA registration number.

(d) The purchaser's name.

(e) The purchaser's complete address.

(f) The purchaser's DEA registration number.

(g) The schedules the purchaser is authorized to receive.

(h) The purchaser's business activity.

(i) The unique tracking number the purchaser assigned to the order.

(j) The date the order was signed.

(k) The name of the controlled substance product.

(l) The National Drug Code (NDC) number of the controlled substance.

(m) The quantity in a single package or container.

(n) The number of packages or containers of each item ordered.

(o) The number of packages or containers shipped.

(p) The date shipped.

2. Part 1311 is added to read as follows:

PART 1311—DIGITAL CERTIFICATES**Subpart A—General**

1311.01 Scope.

1311.02 Definitions.

1311.05 Standards for technologies for electronic transmission of orders.

1311.08 Incorporation by reference.

Subpart B—Obtaining and Using Digital Certificates

1311.10 Eligibility to obtain a digital certificate.

1311.15 Limitations on digital certificates.

1311.16 Coordinators for controlled substances order system digital certificate holders.

1311.20 Requirements for obtaining a digital certificate for signing orders.

1311.30 Requirements for storing and using a private key for digitally signing orders.

1311.40 Number of certificates needed.

1311.45 Renewal of certificates.

1311.50 Requirements for registrants that allow powers of attorney to obtain digital certificates under their DEA registration.

1311.55 Requirements for recipients of digitally signed orders.

1311.60 Requirements for systems used to process digitally signed orders.

1311.65 Recordkeeping.

Authority: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

Subpart A—General**§ 1311.01 Scope.**

This part sets forth the rules governing the use of digital signatures and the protection of private keys by registrants.

§ 1311.02 Definitions.

For the purposes of this chapter:

Biometric authentication means authentication based on measurement of

the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable.

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

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.

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.

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.

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.

FIPS means Federal Information Processing Standards. These Federal standards prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140-2 means a Federal standard for security requirements for cryptographic modules.

FIPS 180-1 means a Federal secure hash standard.

FIPS 186-2 means a Federal standard for applications used to generate and rely upon digital signatures.

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