to receive documents communicated to it via a telecommunications network.

Electronic signature. A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature, and that:

(1) Identifies and authenticates a particular person as the source of the electronic message; and

(2) Indicates such person's approval of the information contained in the electronic message.

Form(s). The term form(s), when used in this part, includes all documents required by 27 CFR, chapter I, to be submitted to TTB.

Handwritten signature. The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other materials or devices that capture the name or mark.

Paper format. A paper document.

TTB. Refers to the Alcohol and Tobacco Tax and Trade Bureau within the Department of the Treasury.

You and I. ''You'' and ''I'' refer to the organization or person who must maintain records or submit documents to TTB to satisfy the requirements of 27 CFR, chapter I.

Subpart B—Electronic Signatures

§ 73.10 What does subpart B cover?

This subpart provides the conditions under which TTB will allow you to use electronic signatures executed to electronic forms instead of traditional handwritten signatures executed on paper forms. Where electronic signatures and their associated electronic forms meet the requirements of this part, TTB will consider the electronic signatures to be the equivalent of full handwritten signatures, initials, and other general signings this chapter requires.

§ 73.11 What are the required components and controls for acceptable electronic signatures?

(a) *Electronic signatures not based on biometrics*. If you use electronic signatures that are not based upon biometrics you must:

(1) Employ at least two distinct identification components such as an identification code and a password;

(2) Use both identification components when executing an electronic signature to an electronic document; and

(3) Ensure that the electronic signature can only be used by the authorized user.

(b) *Electronic signatures based on biometrics*. If you use electronic signatures based upon biometrics, they must be designed to ensure that they cannot be used by anyone other than their genuine owners.

§ 73.12 What security controls must I use for identification codes and passwords?

If you use electronic signatures based upon use of identification codes in combination with passwords, you must employ controls to ensure their security and integrity. These controls must include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password;

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (*e.g.*, to cover such events as password aging);

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, or other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls;

(d) Using transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit and, as appropriate, to organizational management; and