The agency has revised § 11.100 to clarify where and when certificates are to be submitted.

The agency does not agree that the initial certification be provided only upon agency request because FDA believes it is vital to have such certificates, as a matter of record, in advance of any possible litigation. This would clearly establish the intent of organizations to equate the legally binding nature of electronic signatures with traditional handwritten signatures. In addition, the agency believes that having the certification on file ahead of time will have the beneficial effect of reinforcing the gravity of electronic signatures by putting an organization's employees on notice that the organization has gone on record with FDA as equating electronic signatures with handwritten signatures.

121. One comment suggested that proposed § 11.100(c) be revised to exclude from certification instances in which the purported signer claims that he or she did not create or authorize the signature.

The agency declines to make this revision because a provision for nonrepudiation is already contained in § 11.10.

As a result of the considerations discussed in comments 119 and 120 of this document, the agency has revised proposed § 11.100(c) to state that:

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

XII. Electronic Signature Components and Controls (§ 11.200)

122. Proposed § 11.200 sets forth requirements for electronic signature identification mechanisms and controls. Two comments suggested that the term "identification code" should be defined. Several comments suggested that the term "identification mechanisms" should be changed to "identification components" because each component of an electronic signature need not be executed by a different mechanism.

The agency believes that the term "identification code" is sufficiently broad and generally understood and does not need to be defined in these regulations. FDA agrees that the word "component" more accurately reflects the agency's intent than the word "mechanism," and has substituted "component" for "mechanism" in revised § 11.200. The agency has also revised the section heading to read "Electronic signature components and controls" to be consistent with the wording of the section.

123. Proposed § 11.200(a) states that electronic signatures not based upon biometric/behavioral links must: (1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing; (2) be used only by their genuine owners; and (3) be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Two comments said that proposed § 11.200(a) should acknowledge that passwords may be known not only to their genuine owners, but also to system administrators in case people forget their passwords.

The agency does not believe that system administrators would routinely need to know an individual's password because they would have sufficient privileges to assist those individuals who forget passwords.

124. Several comments argued that the agency should accept a single password alone as an electronic signature because: (1) Combining the password with an identification code adds little security, (2) administrative controls and passwords are sufficient, (3) authorized access is more difficult when two components are needed, (4) people would not want to gain unauthorized entry into a manufacturing environment, and (5) changing current systems that use only a password would be costly.

The comments generally addressed the need for two components in electronic signatures within the context of the requirement that all components be used each time an electronic signature is executed. Several comments suggested that, for purposes of system access, individuals should enter both a user identification code and password, but that, for subsequent signings during one period of access, a single element (such as a password) known only to, and usable by, the individual should be sufficient.

The agency believes that it is very important to distinguish between those (nonbiometric) electronic signatures that are executed repetitively during a single, continuous controlled period of time (access session or logged-on period) and those that are not. The agency is concerned, from statements made in comments, that people might use passwords that are not always unique and are frequently words that are easily associated with an individual. Accordingly, where nonbiometric electronic signatures are not executed repetitively during a single, continuous controlled period, it would be extremely bad practice to use a password alone as an electronic signature. The agency believes that using a password alone in such cases would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby easily and readily impersonate that individual. This action could falsify electronic records.

The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a nonbiometric electronic signature for every signing. The agency is persuaded by the comments that such situations generally involve certain conditions. For example, an individual performs an initial system access or "log on," which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password). The individual then performs subsequent signings by executing at least one component of the electronic signature, under controlled conditions that prevent another person from impersonating the legitimate signer. The agency's concern here is the possibility that, if the person leaves the workstation, someone else could access the workstation (or other computer device used to execute the signing) and impersonate the legitimate signer by entering an identification code or password.

The agency believes that, in such situations, it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual.

The agency's objective in accepting the execution of fewer than all the components of a nonbiometric

electronic signature for repetitive signings is to make it impractical to falsify records. The agency believes that this would be attained by complying with all of the following procedures where nonbiometric electronic signatures are executed more than once during a single, continuous controlled session: (1) All electronic signature components are executed for the first signing; (2) at least one electronic signature component is executed at each subsequent signing; (3) the electronic signature component executed after the initial signing is only used by its genuine owner, and is designed to ensure it can only be used by its genuine owner; and (4) the electronic signatures are administered and executed to ensure that their attempted use by anyone other than their genuine owners requires collaboration of two or more individuals. Items 1 and 4 are already incorporated in proposed § 11.200(a). FDA has included items 2 and 3 in final § 11.200(a).

The agency cautions, however, that if its experience with enforcement of part 11 demonstrates that these controls are insufficient to deter falsifications, FDA may propose more stringent controls.

125. One comment asserted that, if the agency intends the term "identification code" to mean the typical user identification, it should not characterize the term as a distinct mechanism because such codes do not necessarily exhibit security attributes. The comment also suggested that proposed § 11.200(a) address the appropriate application of each possible combination of a two-factor authentication method.

The agency acknowledges that the identification code alone does not exhibit security attributes. Security derives from the totality of system controls used to prevent falsification. However, uniqueness of the identification code when combined with another electronic signature component, which may not be unique (such as a password), makes the combination unique and thereby enables a legitimate electronic signature. FDA does not now believe it necessary to address, in § 11.200(a), the application of all possible combinations of multifactored authentication methods.

126. One comment requested clarification of "each signing," noting that a laboratory employee may enter a group of test results under one signing.

The agency advises that each signing means each time an individual executes a signature. Particular requirements regarding what records need to be signed derive from other regulations, not part 11. For example, in the case of a laboratory employee who performs a number of analytical tests, within the context of drug CGMP regulations, it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a)(7)). A separate signing is not required in this context for each separate test as long as the record clearly shows that the single signature means the signer performed all the tests.

127. One comment suggested that the proposed requirement, that collaboration of at least two individuals is needed to prevent attempts at electronic signature falsification, be deleted because a responsible person should be allowed to override the electronic signature of a subordinate. Several comments addressed the phrase "attempted use" and suggested that it be deleted or changed to "unauthorized use." The comments said that willful breaking or circumvention of any security measure does not require two or more people to execute, and that the central question is whether collaboration is required to use the electronic signature.

The agency advises that the intent of the collaboration provision is to require that the components of a nonbiometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token that a person may leave unattended. If an individual must collaborate with another individual by disclosing a password, the risks of betrayal and disclosure are greatly increased and this helps to deter such actions. Because the agency is not condoning such actions, § 11.200(a)(2) requires that electronic signatures be used only by the genuine owner. The agency disagrees with the comments that the term "attempted use" should be changed to "unauthorized uses," because "unauthorized uses" could infer that use of someone else's electronic signature is acceptable if it is authorized.

Regarding electronic signature "overrides," the agency would consider as falsification the act of substituting the signature of a supervisor for that of a subordinate. The electronic signature of the subordinate must remain inviolate for purposes of authentication and documentation. Although supervisors may overrule the actions of their staff, the electronic signatures of the subordinates must remain a permanent part of the record, and the supervisor's own electronic signature must appear separately. The agency believes that such an approach is fully consistent with procedures for paper records.

As a result of the revisions noted in comments 123 to 127 of this document, § 11.200(a) now reads as follows:

(a) Electronic signatures that are not based upon biometrics shall:

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

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

128. Proposed § 11.200(b) states that electronic signatures based upon biometric/behavioral links be designed to ensure that they could not be used by anyone other than their genuine owners.

One comment suggested that the agency make available, by public workshop or other means, any information it has regarding existing biometric systems so that industry can provide proper input. Another comment asserted that proposed § 11.200(b) placed too great an emphasis on biometrics, did not establish particular levels of assurance for biometrics, and did not provide for systems using mixtures of biometric and nonbiometric electronic signatures. The comment recommended revising the phrase "designed to ensure they cannot be used" to read "provide assurances that prevent their execution."

The agency's experience with biometric electronic signatures is contained in the administrative record for this rulemaking, under docket no. 92N-0251, and includes recommendations from public comments to the ANPRM and the proposed rule. The agency has also gathered, and continues to gather, additional information from literature reviews, general press reports, meetings, and the agency's experience with this technology. Interested persons have had extensive opportunity for input and comment regarding biometrics in part 11. In addition, interested persons may continue to contact the agency at any time regarding biometrics or any other relevant technologies. The agency notes

that the rule does not require the use of biometric-based electronic signatures.

As the agency's experience with biometric electronic signatures increases, FDA will consider holding or participating in public workshops if that approach would be helpful to those wishing to adopt such technologies to comply with part 11.

The agency does not believe that proposed § 11.200(b) places too much emphasis on biometric electronic signatures. As discussed above, the regulation makes a clear distinction between electronic signatures that are and are not based on biometrics, but treats their acceptance equally.

The agency recognizes the inherent security advantages of biometrics, however, in that record falsification is more difficult to perform. System controls needed to make biometric-based electronic signatures reliable and trustworthy are thus different in certain respects from controls needed to make nonbiometric electronic signatures reliable and trustworthy. The requirements in part 11 reflect those differences.

The agency does not believe that it is necessary at this time to set numerical security assurance standards that any system would have to meet.

The regulation does not prohibit individuals from using combinations of biometric and nonbiometric-based electronic signatures. However, when combinations are used, FDA advises that requirements for each element in the combination would also apply. For example, if passwords are used in combination with biometrics, then the benefits of using passwords would only be realized, in the agency's view, by adhering to controls that ensure password integrity (see § 11.300).

In addition, the agency believes that the phrase "designed to ensure that they cannot be used" more accurately reflects the agency's intent than the suggested alternate wording, and is more consistent with the concept of systems validation. Under such validation, falsification preventive attributes would be designed into the biometric systems.

To be consistent with the revised definition of biometrics in § 11.3(b)(3), the agency has revised § 11.200(b) to read, "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."

XIII. Electronic Signatures—Controls for Identification Codes/Passwords (§ 11.300)

The introductory paragraph of proposed § 11.300 states that electronic signatures based upon use of identification codes in combination with passwords must employ controls to ensure their security and integrity.

To clarify the intent of this provision, the agency has added the words "[p]ersons who use" to the first sentence of § 11.300. This change is consistent with §§ 11.10 and 11.30. The introductory paragraph now reads, "Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: * * *."

129. One comment suggested deletion of the phrase "in combination with passwords" from the first sentence of this section.

The agency disagrees with the suggested revision because the change is inconsistent with FDA's intent to address controls for electronic signatures based on combinations of identification codes and passwords, and would, in effect, permit a single component nonbiometric-based electronic signature.

130. Proposed § 11.300(a) states that controls for identification codes/passwords must include maintaining the uniqueness of each issuance of identification code and password.

One comment alleged that most passwords are commonly used words, such as a child's name, a State, city, street, month, holiday, or date, that are significant to the person who creates the password. Another stated that the rule should explain uniqueness and distinguish between issuance and use because identification code/password combinations generally do not change for each use.

FDA does not intend to require that individuals use a completely different identification code/password combination each time they execute an electronic signature. For reasons explained in the response to comment 16, what is required to be unique is each combined password and identification code and FDA has revised the wording of § 11.300(a) to clarify this provision. The agency is aware, however, of identification devices that generate new passwords on a continuous basis in synchronization with a "host" computer. This results in unique passwords for each system access. Thus, it is possible in theory to generate a unique nonbiometric electronic signature for each signing.

The agency cautions against using passwords that are common words easily associated with their originators because such a practice would make it relatively easy for someone to impersonate someone else by guessing the password and combining it with an unsecured (or even commonly known) identification code.

131. Proposed § 11.300(b) states that controls for identification codes/passwords must ensure that code/password issuances are periodically checked, recalled, or revised.

Several comments objected to this proposed requirement because: (1) It is unnecessary, (2) it excessively prescribes "how to," (3) it duplicates the requirements in § 11.300(c), and (4) it is administratively impractical for larger organizations. However, the comments said individuals should be encouraged to change their passwords periodically. Several comments suggested that proposed § 11.300(b) include a clarifying example such as "to cover events such as password aging." One comment said that the section should indicate who is to perform the periodic checking, recalling, or revising.

The agency disagrees with the objections to this provision. FDA does not view the provision as a "how to" because organizations have full flexibility in determining the frequency and methods of checking, recalling, or revising their code/password issuances. The agency does not believe that this paragraph duplicates the regulation in § 11.300(c) because paragraph (c) specifically addresses followup to losses of electronic signature issuances, whereas § 11.300(b) addresses periodic issuance changes to ensure against their having been unknowingly compromised. This provision would be met by ensuring that people change their passwords periodically.

FDA disagrees that this system control is unnecessary or impractical in large organizations because the presence of more people may increase the opportunities for compromising identification codes/passwords. The agency is confident that larger organizations will be fully capable of handling periodic issuance checks, revisions, or recalls.

FDA agrees with the comments that suggested a clarifying example and has revised § 11.300(b) to include password aging as such an example. The agency cautions, however, that the example should not be taken to mean that password expiration would be the only rationale for revising, recalling, and checking issuances. If, for example, identification codes and passwords have been copied or compromised, they should be changed.

FDA does not believe it necessary at this time to specify who in an organization is to carry out this system control, although the agency expects

that units that issue electronic signatures would likely have this duty.

132. Proposed § 11.300(c) states that controls for identification codes/passwords must include the following of loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.

One comment suggested that this section be deleted because it excessively prescribes "how to." Another comment argued that the proposal was not detailed enough and should distinguish among fundamental types of cards (e.g., magstripe, integrated circuit, and optical) and include separate sections that address their respective use. Two comments questioned why the proposal called for "rigorous controls" in this section as opposed to other sections. One of the comments recommended that this section should also apply to cards or devices that are stolen as well as lost.

The agency believes that the requirement that organizations institute loss management procedures is neither too detailed nor too general. Organizations retain full flexibility in establishing the details of such procedures. The agency does not believe it necessary at this time to offer specific provisions relating to different types of cards or tokens. Organizations that use such devices retain full flexibility to establish appropriate controls for their operations. To clarify the agency's broad intent to cover all types of devices that contain or generate identification code or password information, FDA has revised § 11.300(c) to replace "etc." with "and other devices that bear or generate identification code or password information."

The agency agrees that § 11.300(c) should cover loss management procedures regardless of how devices become potentially compromised, and has revised this section by adding, after the word "lost," the phrase "stolen, missing, or otherwise potentially compromised." FDA uses the term "rigorous" because device disappearance may be the result of inadequate controls over the issuance and management of the original cards or devices, thus necessitating more stringent measures to prevent problem recurrence. For example, personnel training on device safekeeping may need to be strengthened.

133. Proposed § 11.300(d) states that controls for identification codes/passwords must include the use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and, detecting and reporting to the system security unit and organizational management in an emergent manner any attempts at their unauthorized use.

Several comments suggested that the term "emergent" in proposed § 11.300(d) be replaced with "timely" to describe reports regarding attempted unauthorized use of identification codes/passwords because: (1) A timely report would be sufficient, (2) technology to report emergently is not available, and (3) timely is a more recognizable and common term.

FDA agrees in part. The agency considers attempts at unauthorized use of identification codes and passwords to be extremely serious because such attempts signal potential electronic signature and electronic record falsification, data corruption, or worse—consequences that could also ultimately be very costly to organizations. In FDA's view, the significance of such attempts requires the immediate and urgent attention of appropriate security personnel in the same manner that individuals would respond to a fire alarm. To clarify its intent with a more widely recognized term, the agency is replacing "emergent" with "immediate and urgent" in the final rule. The agency believes that the same technology that accepts or rejects an identification code and password can be used to relay to security personnel an appropriate message regarding attempted misuse.

134. One comment suggested that the word "any" be deleted from the phrase "any attempts" in proposed § 11.300(d) because it is excessive. Another comment, noting that the question of attempts to enter a system or access a file by unauthorized personnel is very serious, urged the agency to substitute "all" for "any." This comment added that there are devices on the market that can be used by unauthorized individuals to locate personal identification codes and passwords.

The agency believes the word "any" is sufficiently broad to cover all attempts at misuse of identification codes and passwords, and rejects the suggestion to delete the word. If the word "any" were deleted, laxity could result from any inference that persons are less likely to be caught in an essentially permissive, nonvigilant system. FDA is aware of the "sniffing" devices referred to by one comment and cautions persons to establish suitable countermeasures against them.

135. One comment suggested that proposed § 11.300(d) be deleted because it is impractical, especially when simple typing errors are made. Another suggested that this section pertain to access to electronic records, not just the system, on the basis that simple miskeys may be typed when accessing a system.

As discussed in comments 133 and 134 of this document, the agency believes this provision is necessary and reasonable. The agency's security concerns extend to system as well as record access. Once having gained unauthorized system access, an individual could conceivably alter passwords to mask further intrusion and misdeeds. If this section were removed, falsifications would be more probable to the extent that some establishments would not alert security personnel.

However, the agency advises that a simple typing error may not indicate an unauthorized use attempt, although a pattern of such errors, especially in short succession, or such an apparent error executed when the individual who "owns" that identification code or password is deceased, absent, or otherwise known to be unavailable, could signal a security problem that should not be ignored. FDA notes that this section offers organizations maximum latitude in deciding what they perceive to be attempts at unauthorized use.

136. One comment suggested substituting the phrase "electronic signature" for "passwords and/or identification codes."

The agency disagrees with this comment because the net effect of the revision might be to ignore attempted misuse of important elements of an electronic signature such as a "password" attack on a system.

137. Several comments argued that: (1) It is not necessary to report misuse attempts simultaneously to management when reporting to the appropriate security unit, (2) security units would respond to management in accordance with their established procedures and lines of authority, and (3) management would not always be involved.

The agency agrees that not every misuse attempt would have to be reported simultaneously to an organization's management if the security unit that was alerted responded appropriately. FDA notes, however, that some apparent security breeches could be serious enough to warrant management's immediate and urgent attention. The agency has revised proposed § 11.300(d) to give organizations maximum flexibility in establishing criteria for management notification. Accordingly, § 11.300(d) now states that controls for identification codes/passwords must include:

Use of 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.

138. Proposed § 11.300(e) states that controls for identification codes/passwords must include initial and periodic testing of devices, such as tokens or cards, bearing identifying information, for proper function.

Many comments objected to this proposed device testing requirement as unnecessary because it is part of system validation and because devices are access fail-safe in that nonworking devices would deny rather than permit system access. The comments suggested revising this section to require that failed devices deny user access. One comment stated that § 11.300(e) is unclear on the meaning of "identifying information" and that the phrase "tokens or cards" is redundant because cards are a form of tokens.

FDA wishes to clarify the reason for this proposed requirement, and to emphasize that proper device functioning includes, in addition to system access, the correctness of the identifying information and security performance attributes. Testing for system access alone could fail to discern significant unauthorized device alterations. If, for example, a device has been modified to change the identifying information, system access may still be allowed, which would enable someone to assume the identity of another person. In addition, devices may have been changed to grant individuals additional system privileges and action authorizations beyond those granted by the organization. Of lesser significance would be simple wear and tear on such devices, which result in reduced performance. For instance, a bar code may not be read with the same consistent accuracy as intended if the code becomes marred, stained, or otherwise disfigured. Access may be granted, but only after many more scannings than desired. The agency expects that device testing would detect such defects.

Because validation of electronic signature systems would not cover unauthorized device modifications, or subsequent wear and tear, validation would not obviate the need for periodic testing.

The agency notes that § 11.300(e) does not limit the types of devices organizations may use. In addition, not all tokens may be cards, and identifying information is intended to include identification codes and passwords. Therefore, FDA has revised proposed § 11.300(e) to clarify the agency's intent and to be consistent with § 11.300(c). Revised § 11.300(e) requires initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

XIV. Paperwork Reduction Act of 1995

This final rule contains information collection provisions that are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520). Therefore, in accordance with 5 CFR 1320, the title, description, and description of respondents of the collection of information requirements are shown below with an estimate of the annual reporting and recordkeeping burdens. Included in the estimate is the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Most of the burden created by the information collection provision of this final rule will be a one-time burden associated with the creation of standard operating procedures, validation, and certification. The agency anticipates the use of electronic media will substantially reduce the paperwork burden associated with maintaining FDA-required records.

Title: Electronic records; Electronic signatures.

Description: FDA is issuing regulations that provide criteria for acceptance of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records. Rules apply to any FDA records requirements unless specific restrictions are issued in the future. Records required to be submitted to FDA may be submitted electronically, provided the agency has stated its ability to accept the records electronically in an agency established public docket.

Description of Respondents: Businesses and other for-profit organizations, state or local governments, Federal agencies, and nonprofit institutions.

Although the August 31, 1994, proposed rule (59 FR 45160) provided a 90-day comment period under the Paperwork Reduction Act of 1980, FDA is providing an additional opportunity for public comment under the Paperwork Reduction Act of 1995, which was enacted after the expiration of the comment period and applies to this final rule. Therefore, FDA now invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of FDA's functions, including whether the information will have practical utility; (2) the accuracy of FDA's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques, when appropriate, and other forms of information technology. Individuals and organizations may submit comments on the information collection provisions of this final rule by May 19, 1997. Comments should be directed to the Dockets Management Branch (address above).

At the close of the 60-day comment period, FDA will review the comments received, revise the information collection provisions as necessary, and submit these provisions to OMB for review and approval. FDA will publish a notice in the Federal Register when the information collection provisions are submitted to OMB, and an opportunity for public comment to OMB will be provided at that time. Prior to the effective date of this final rule, FDA will publish a notice in the Federal Register of OMB's decision to approve, modify, or disapprove the information collection provisions. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

TABLE 1.—ESTIMATED ANNUAL RECORDKEEPING BURDEN

21 CFR Section	Annual No. of Recordkeepers	Hours per Recordkeeper	Total Hours
11.10	50	40	2,000
11.30	50	40	2,000
11.50	50	40	2,000

TABLE 1.—ESTIMATED ANNUAL RECORDKEEPING BURDEN—Continued

21 CFR Section	Annual No. of Recordkeepers	Hours per Recordkeeper	Total Hours
11.300	50	40	2,000
Total annual burden hours			8,000

TABLE 2.—ESTIMATED ANNUAL REPORTING BURDEN

21 CFR Section	Annual No. of Respondents	Hours per Response	Total Burden Hours
11.100	1,000	1	1,000
Total annual burden hours			1,000

XV. Environmental Impact

The agency has determined under 21 CFR 25.24(a)(8) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

XVI. Analysis of Impacts

FDA has examined the impacts of the final rule under Executive Order 12866, under the Regulatory Flexibility Act (5 U.S.C. 601–612), and under the Unfunded Mandates Reform Act (Pub. L. 104–4). Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; and distributive impacts and equity). Unless an agency certifies that a rule will not have a significant economic impact on a substantial number of small entities, the Regulatory Flexibility Act requires an analysis of regulatory options that would minimize any significant impact of a rule on small entities. The Unfunded Mandates Reform Act requires that agencies prepare an assessment of anticipated costs and benefits before proposing any rule that may result in an annual expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million (adjusted annually for inflation).

The agency believes that this final rule is consistent with the regulatory philosophy and principles identified in the Executive Order. This rule permits persons to maintain any FDA required record or report in electronic format. It also permits FDA to accept electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. The rule applies to any paper records required by statute or agency regulations. The rule was substantially influenced by comments to the ANPRM and the proposed rule. The provisions of this rule permit the use of electronic technology under conditions that the agency believes are necessary to ensure the integrity of electronic systems, records, and signatures, and the ability of the agency to protect and promote the public health.

This rule is a significant regulatory action as defined by the Executive Order and is subject to review under the Executive Order. This rule does not impose any mandates on State, local, or tribal governments, nor is it a significant regulatory action under the Unfunded Mandates Reform Act.

The activities regulated by this rule are voluntary; no entity is required by this rule to maintain or submit records electronically if it does not wish to do so. Presumably, no firm (or other regulated entity) will implement electronic recordkeeping unless the benefits to that firm are expected to exceed any costs (including capital and maintenance costs). Thus, the industry will incur no net costs as a result of this rule.

Based on the fact that the activities regulated by this rule are entirely voluntary and will not have any net adverse effects on small entities, the Commissioner of Food and Drugs certifies that this rule will not have a significant economic impact on a substantial number of small entities. Therefore, under the Regulatory Flexibility Act, no further regulatory flexibility analysis is required.

Although no further analysis is required, in developing this rule, FDA has considered the impact of the rule on small entities. The agency has also considered various regulatory options to maximize the net benefits of the rule to small entities without compromising the integrity of electronic systems, records, and signatures, or the agency's ability to protect and promote the public health. The following analysis briefly examines the potential impact of this rule on small businesses and other small entities, and describes the measures that FDA incorporated in this final rule to reduce the costs of applying electronic record/signature systems consistent with the objectives of the rule. This analysis includes each of the elements required for a final regulatory flexibility analysis under 5 U.S.C. 604(a).

A. Objectives

The purpose of this rule is to permit the use of a technology that was not contemplated when most existing FDA regulations were written, without undermining in any way the integrity of records and reports or the ability of FDA to carry out its statutory health protection mandate. The rule will permit regulated industry and FDA to operate with greater flexibility, in ways that will improve both the efficiency and the speed of industry's operations and the regulatory process. At the same time, it ensures that individuals will assign the same level of importance to affixing an electronic signature, and the records to which that signature attests, as they currently do to a handwritten signature.

B. Small Entities Affected

This rule potentially affects all large and small entities that are required by any statute administered by FDA, or any FDA regulation, to keep records or make reports or other submissions to FDA, including small businesses, nonprofit organizations, and small government entities. Because the rule affects such a broad range of industries, no data currently exist to estimate precisely the total number of small entities that will potentially benefit from the rule, but the number is substantial. For example, within the medical devices industry alone, the Small Business