necessary" and argued that validation of commercially available software is not necessary because such software has already been thoroughly validated. The comment acknowledged that validation may be required for application programs written by manufacturers and others for special needs.

The agency disagrees with the comment's claim that all commercial software has been validated. The agency believes that commercial availability is no guarantee that software has undergone "thorough validation" and is unaware of any regulatory entity that has jurisdiction over general purpose software producers. The agency notes that, in general, commercial software packages are accompanied not by statements of suitability or compliance with established standards, but rather by disclaimers as to their fitness for use. The agency is aware of the complex and sometimes controversial issues in validating commercial software. However, the need to validate such software is not diminished by the fact that it was not written by those who will use the software.

In the future, the agency may provide guidance on validation of commercial software used in electronic record systems. FDA has addressed the matter of software validation in general in such documents as the "Draft Guideline for the Validation of Blood Establishment Computer Systems," which is available from the Manufacturers Assistance and Communications Staff, Center for Biologics Evaluation and Research (HFM-42), Food and Drug Administration, 1401 Rockville Pike, Rockville, MD 20852-1448, 301-594-2000. This guideline is also available by sending e-mail to the following Internet address: CBER_INFO@A1.CBER.FDA.GOV). For the purposes of part 11, however, the agency believes it is vital to retain the validation requirement.

66. One comment requested an explanation of what was meant by the phrase "consistent intended" in proposed § 11.10(a) and why "consistent performance" was not used instead. The comment suggested that the rule should distinguish consistent intended performance from well-recognized service "availability."

The agency advises that the phrase "consistent intended performance" relates to the general principle of validation that planned and expected performance is based upon predetermined design specifications (hence, "intended"). This concept is in accord with the agency's 1987 "Guideline on General Principles of Process Validation," which is available from the Division of Manufacturing and Product Quality, Center for Drug Evaluation and Research (HFD-320), Food and Drug Administration, 7520 Standish Pl., Rockville, MD 20855, 301-594-0093). This guideline defines validation as establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes. The agency believes that the comment's concepts are accommodated by this definition to the extent that system "availability" may be one of the predetermined specifications or quality attributes.

67. One comment said the rule should indicate whether validation of systems does, or should, require any certification or accreditation.

The agency believes that although certification or accreditation may be a part of validation of some systems, such certification or accreditation is not necessary in all cases, outside of the context of any such approvals within an organization itself. Therefore, part 11 is silent on the matter.

68. One comment said the rule should clarify whether system validation should be capable of discerning the absence of electronic records, in light of agency concerns about falsification. The comment added that the agency's concerns regarding invalid or altered records can be mitigated by use of cryptographically enhanced methods, including secure time and date stamping.

The agency does not believe that it is necessary at this time to include an explicit requirement that systems be capable of detecting the absence of records. The agency advises that the requirement in § 11.10(e) for audit trails of operator actions would cover those actions intended to delete records. Thus, the agency would expect firms to document such deletions, and would expect the audit trail mechanisms to be included in the validation of the electronic records system.

69. Proposed § 11.10(b) states that controls for closed systems must include the ability to generate true copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency, and that if there were any questions regarding the ability of the agency to perform such review and copying, persons should contact the agency.

Several comments objected to the requirement for "true" copies of electronic records. The comments asserted that information in an original record (as may be contained in a database) may be presented in a copy in a different format that may be more usable. The comments concluded that, to generate precise "true" copies of electronic records, firms may have to retain the hardware and software that had been used to create those records in the first place (even when such hardware and software had been replaced by newer systems). The comments pointed out that firms may have to provide FDA with the application logic for "true" copies, and that this may violate copyright provisions. One comment illustrated the difference between "true" copies and other equally reliable, but not exact, copies of electronic records by noting that pages from FDA's paper publications (such as the CFR and the Compliance Policy Guidance Manual) look quite different from electronic copies posted to FDA's bulletin board. The comments suggested different wording that would effectively require accurate and complete copies, but not necessarily "true" copies.

The agency agrees that providing exact copies of electronic records in the strictest meaning of the word "true" may not always be feasible. The agency nonetheless believes it is vital that copies of electronic records provided to FDA be accurate and complete. Accordingly, in § 11.10(b), "true" has been replaced with "accurate and complete." The agency expects that this revision should obviate the potential problems noted in the comments. The revision should also reduce the costs of providing copies by making clear that firms need not maintain obsolete equipment in order to make copies that are "true" with respect to format and computer system.

70. Many comments objected to the proposed requirement that systems be capable of generating electronic copies of electronic records for FDA inspection and copying, although they generally agreed that it was appropriate to provide FDA with readable paper copies. Alternative wording was suggested that would make providing electronic copies optional, such that persons could provide FDA with nothing but paper copies if they so wished. The comments argued that providing FDA with electronic copies was unnecessary, unjustified, not practical considering the different types of computer systems that may be in use, and would unfairly limit firms in their selection of hardware and software if they could only use systems that matched FDA's capabilities (capabilities which, it was argued, would not be uniform throughout the United States). One comment suggested that the rule specify

a particular format, such as ASCII, for electronic copies to FDA.

The agency disagrees with the assertion that FDA need only be provided with paper copies of electronic records. To operate effectively, the agency must function on the same technological plane as the industries it regulates. Just as firms realize efficiencies and benefits in the use of electronic records, FDA should be able to conduct audits efficiently and thoroughly using the same technology. For example, where firms perform computerized trend analyses of electronic records to improve their processes, FDA should be able to use computerized methods to audit electronic records (on site and off, as necessary) to detect trends, inconsistencies, and potential problem areas. If FDA is restricted to reviewing only paper copies of those records, the results would severely impede its operations. Inspections would take longer to complete, resulting in delays in approvals of new medical products, and expenditure of additional resources both by FDA (in performing the inspections and transcribing paper records to electronic format) and by the inspected firms, which would generate the paper copies and respond to questions during the resulting lengthened inspections.

The agency believes that it also may be necessary to require that persons furnish certain electronic copies of electronic records to FDA because paper copies may not be accurate and complete if they lack certain audit trail (metadata) information. Such information may have a direct bearing on record trustworthiness and reliability. These data could include information, for example, on when certain items of electronic mail were sent and received.

The agency notes that people who use different computer systems routinely provide each other with electronic copies of electronic records, and there are many current and developing tools to enable such sharing. For example, at a basic level, records may be created in, or transferred to, the ASCII format. Many different commercial programs have the capability to import from, and export to, electronic records having different formats. Firms use electronic data interchange (commonly known as EDI) and agreed upon transaction set formats to enable them to exchange copies of electronic records effectively. Third parties are also developing portable document formats to enable conversion among several diverse formats.

Concerning the ability of FDA to handle different formats of electronic records, based upon the emergence of format conversion tools such as those mentioned above, the agency's experience with electronic submissions such as computer assisted new drug applications (commonly known as CANDA's), and the agency's planned Submissions Management and Review Tracking System (commonly known as SMART), FDA is confident that it can work with firms to minimize any formatting difficulties. In addition, substitution of the words "accurate and complete" for "true," as discussed in comment 69, should make it easier for firms to provide FDA with electronic copies of their electronic records. FDA does not believe it is necessary to specify any particular format in part 11 because it prefers, at this time, to afford industry and the agency more flexibility in deciding which formats meet the capabilities of all parties. Accordingly, the agency has revised proposed § 11.10(b) to read:

> The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

71. Proposed § 11.10(c) states that procedures and controls for closed systems must include the protection of records to enable their accurate and ready retrieval throughout the records retention period.

One firm commented that, because it replaces systems often (about every 3 years), it may have to retain supplanted systems to meet these requirements. Another comment suggested that the rule be modified to require records retention only for as long as "legally mandated."

The agency notes that, as discussed in comment 70 of this document, persons would not necessarily have to retain supplanted hardware and software systems provided they implemented conversion capabilities when switching to replacement technologies. The agency does not believe it is necessary to add the qualifier "legally mandated" because the retention period for a given record will generally be established by the regulation that requires the record. Where the regulations do not specify a given time, the agency would expect firms to establish their own retention periods. Regardless of the basis for the retention period, FDA believes that the requirement that a given electronic record be protected to permit it to be accurately and readily retrieved for as long as it is kept is reasonable and necessary.

72. Proposed § 11.10(e) would require the use of time-stamped audit trails to document record changes, all write-to-file operations, and to independently record the date and time of operator entries and actions. Record changes must not obscure previously recorded information and such audit trail documentation must be retained for a period at least as long as required for the subject electronic documents and must be available for agency review and copying.

Many comments objected to the proposed requirement that all write-to-file operations be documented in the audit trail because it is unnecessary to document all such operations. The comments said that this would require audit trails for such automated recordings as those made to internal buffers, data swap files, or temporary files created by word processing programs. The comments suggested revising § 11.10(e) to require audit trails only for operator entries and actions.

Other comments suggested that audit trails should cover: (1) Operator data inputs but not actions, (2) only operator changes to records, (3) only critical write-to-file information, (4) operator changes as well as all actions, (5) only new entries, (6) only systems where data can be altered, (7) only information recorded by humans, (8) information recorded by both humans and devices, and (9) only entries made upon adoption of the records as official. One comment said audit trails should not be required for data acquisition systems, while another comment said audit trails are critical for data acquisition systems.

It is the agency's intent that the audit trail provide a record of essentially who did what, wrote what, and when. The write-to-file operations referenced in the proposed rule were not intended to cover the kind of "background" nonhuman recordings the comments identified.

The agency considers such operator actions as activating a manufacturing sequence or turning off an alarm to warrant the same audit trail coverage as operator data entries in order to document a thorough history of events and those responsible for such events. Although FDA acknowledges that not every operator "action," such as switching among screen displays, need be covered by audit trails, the agency is concerned that revising the rule to cover only "critical" operations would result in excluding much information and actions that are necessary to document events thoroughly.

The agency believes that, in general, the kinds of operator actions that need to be covered by an audit trail are those important enough to memorialize in the electronic record itself. These are actions which, for the most part, would be recorded in corresponding paper records according to existing recordkeeping requirements.

The agency intends that the audit trail capture operator actions (e.g., a command to open a valve) at the time they occur, and operator information (e.g., data entry) at the time the information is saved to the recording media (such as disk or tape), in much the same manner as such actions and information are memorialized on paper. The audit trail need not capture every keystroke and mistake that is held in a temporary buffer before those commitments. For example, where an operator records the lot number of an ingredient by typing the lot number, followed by the "return key" (where pressing the return key would cause the information to be saved to a disk file), the audit trail need not record every "backspace delete" key the operator may have previously pressed to correct a typing error. Subsequent "saved" corrections made after such a commitment, however, must be part of the audit trail.

At this time, the agency's primary concern relates to the integrity of human actions. Should the agency's experience with part 11 demonstrate a need to require audit trails of device operations and entries, the agency will propose appropriate revisions to these regulations. Accordingly, the agency has revised proposed § 11.10(e) by removing reference to all write-to-file operations and clarifying that the audit trail is to cover operator entries and actions that create, modify, or delete electronic records.

73. A number of comments questioned whether proposed § 11.10(e) mandated that the audit trail be part of the electronic record itself or be kept as a separate record. Some comments interpreted the word "independently" as requiring a separate record. Several comments focused on the question of whether audit trails should be generated manually under operator control or automatically without operator control. One comment suggested a revision that would require audit trails to be generated by computer, because the system, not the operator, should record the audit trail. Other comments said the rule should facilitate date and time recording by software, not operators, and that the qualifier "securely" be added to the language describing the audit trail. One comment, noting that audit trails require validation and qualification to ensure that time stamps are accurate and independent, suggested that audit trails be required only when operator actions are witnessed.

The agency advises that audit trail information may be contained as part of the electronic record itself or as a separate record. FDA does not intend to require one method over the other. The word "independently" is intended to require that the audit trail not be under the control of the operator and, to prevent ready alteration, that it be created independently of the operator.

To maintain audit trail integrity, the agency believes it is vital that the audit trail be created by the computer system independently of operators. The agency believes it would defeat the purpose of audit trails to permit operators to write or change them. The agency believes that, at this time, the source of such independent audit trails may effectively be within the organization that creates the electronic record. However, the agency is aware of a situation under which time and date stamps are provided by trusted third parties outside of the creating organization. These third parties provide, in effect, a public electronic notary service. FDA will monitor development of such services in light of part 11 to determine if a requirement for such third party services should be included in these regulations. For now, the agency considers the advent of such services as recognition of the need for strict objectivity in recording time and date stamps.

The agency disagrees with the premise that only witnessed operator actions need be covered by audit trails because the opportunities for record falsification are not limited to cases where operator actions are witnessed. Also, the need for validating audit trails does not diminish the need for their implementation.

FDA agrees with the suggestion that the proposed rule be revised to require a secure audit trail—a concept inherent in having such a control at all. Accordingly, proposed § 11.10(e) has been revised to require use of "secure, computer-generated" audit trails.

74. A few comments objected to the requirement that time be recorded, in addition to dates, and suggested that time be recorded only when necessary and feasible. Other comments specifically supported the requirement for recording time, noting that time stamps make electronic signatures less vulnerable to fraud and abuse. The comments noted that, in any setting, there is a need to identify the date, time, and person responsible for adding to or changing a value. One of the comments suggested that the rule require recording the reason for making changes to electronic records. Other comments implicitly supported recording time.

FDA believes that recording time is a critical element in documenting a sequence of events. Within a given day a number of events and operator actions may take place, and without recording time, documentation of those events would be incomplete. For example, without time stamps, it may be nearly impossible to determine such important sequencing as document approvals and revisions and the addition of ingredients in drug production. Thus, the element of time becomes vital to establishing an electronic record's trustworthiness and reliability.

The agency notes that comments on the ANPRM frequently identified use of date/time stamps as an important system control. Time recording, in the agency's view, can also be an effective deterrent to records falsification. For example, event sequence codes alone would not necessarily document true time in a series of events, making falsification of that sequence easier if time stamps are not used. The agency believes it should be very easy for firms to implement time stamps because there is a clock in every computer and document management software, electronic mail systems and other electronic record/electronic applications, such as digital signature programs, commonly apply date and time stamps. The agency does not intend that new technologies, such as cryptographic technologies, will be needed to comply with this requirement. The agency believes that implementation of time stamps should be feasible in virtually all computer systems because effective computer operations depend upon internal clock or timing mechanisms and, in the agency's experience, most computer systems are capable of precisely recording such time entries as when records are saved.

The agency is implementing the time stamp requirement based on the understanding that all current computers, electronic document software, electronic mail, and related electronic record systems include such technologies. The agency also understands that time stamps are applied automatically by these systems, meaning firms would not have to install additional hardware, software, or incur additional burden to implement this control. In recognition of this, the agency wishes to clarify that a primary intent of this provision is to ensure that people take reasonable measures to

ensure that those built in time stamps are accurate and that people do not alter them casually so as to readily mask unauthorized record changes.

The agency advises that, although part 11 does not specify the time units (e.g., tenth of a second, or even the second) to be used, the agency expects the unit of time to be meaningful in terms of documenting human actions.

The agency does not believe part 11 needs to require recording the reason for record changes because such a requirement, when needed, is already in place in existing regulations that pertain to the records themselves.

75. One comment stated that proposed § 11.10(e) should not require an electronic signature for each write-to-file operation.

The agency advises that § 11.10(e) does not require an electronic signature as the means of authenticating each write-to-file operation. The agency expects the audit trail to document who did what and when, documentation that can be recorded without electronic signatures themselves.

76. Several comments, addressing the proposed requirement that record changes not obscure previously recorded information, suggested revising proposed § 11.10(e) to apply only to those entries intended to update previous information.

The agency disagrees with the suggested revision because the rewording is too narrow. The agency believes that some record changes may not be "updates" but significant modifications or falsifications disguised as updates. All changes to existing records need to be documented, regardless of the reason, to maintain a complete and accurate history, to document individual responsibility, and to enable detection of record falsifications.

77. Several comments suggested replacing the word "document" with "record" in the phrase "Such audit trails shall be retained for a period at least as long as required for the subject electronic documents * * *" because not all electronic documents are electronic records and because the word document connotes paper.

As discussed in section III.D. of this document, the agency equates electronic documents with electronic records, but for consistency, has changed the phrase to read "Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records * * *."

78. Proposed § 11.10(k)(ii) (§ 11.10(k)(2) in this regulation) addresses electronic audit trails as a systems documentation control. One comment noted that this provision appears to be the same as the audit trail provision of proposed § 11.10(e) and requested clarification.

The agency wishes to clarify that the kinds of records subject to audit trails in the two provisions cited by the comment are different. Section 11.10(e) pertains to those records that are required by existing regulations whereas § 11.10(k)(2) covers the system documentation records regarding overall controls (such as access privilege logs, or system operational specification diagrams). Accordingly, the first sentence of § 11.10(e) has been revised to read "Use of secure, computer-generated, time-stamped audit trails to independently record and date the time of operator entries and actions that create, modify, or delete electronic records."

79. Proposed § 11.10(f) states that procedures and controls for closed systems must include the use of operational checks to enforce permitted sequencing of events, as appropriate.

Two comments requested clarification of the agency's intent regarding operational checks.

The agency advises that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization.

80. Several comments suggested that, for clarity, the phrase "operational checks" be modified to "operational system checks."

The agency agrees that the added modifier "system" more accurately reflects the agency's intent that operational checks be performed by the computer systems and has revised proposed § 11.10(f) accordingly.

81. Several comments suggested revising proposed § 11.10(f) to clarify what is to be checked. The comments suggested that "steps" in addition to "events" be checked, only critical steps be checked, and that "records" also be checked.

The agency intends the word "event" to include "steps" such as production steps. For clarity, however, the agency has revised proposed § 11.10(f) by adding the word "steps." The agency does not, however, agree that only critical steps need be subject to operational checks because a given specific step or event may not be critical, yet it may be very important that the step be executed at the proper time relative to other steps or events. The agency does not believe it necessary to add the modifier "records" to proposed § 11.10(f) because creation, deletion, or modification of a record is an event. Should it be necessary to create, delete, or modify records in a particular sequence, operational system checks would ensure that the proper sequence is followed.

82. Proposed § 11.10(g) states that procedures and controls for closed systems must include the use of authority checks to ensure that only authorized individuals use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

One comment suggested that the requirement for authority checks be qualified with the phrase "as appropriate," on the basis that it would not be necessary for certain parts of a system, such as those not affecting an electronic record. The comment cited pushing an emergency stop button as an example of an event that would not require an authority check. Another comment suggested deleting the requirement on the basis that some records can be read by all employees in an organization.

The agency advises that authority checks, and other controls under § 11.10, are intended to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that signers cannot readily repudiate a signed record as not genuine. Functions outside of this context, such as pressing an emergency stop button, would not be covered. However, even in this example, the agency finds it doubtful that a firm would permit anyone, such as a stranger from outside the organization, to enter a facility and press the stop button at will regardless of the existence of an emergency. Thus, there would likely be some generalized authority checks built into the firm's operations.

The agency believes that few organizations freely permit anyone from within or without the operation to use their computer system, electronically sign a record, access workstations, alter records, or perform operations. It is likely that authority checks shape the activities of almost every organization. The nature, scope, and mechanism of performing such checks is up to the operating organization. FDA believes, however, that performing such checks is one of the most fundamental measures to ensure the integrity and trustworthiness of electronic records.

Proposed § 11.10(g) does not preclude all employees from being permitted to read certain electronic records. However, the fact that some records may be read by all employees would not

justify deleting the requirement for authority checks entirely. The agency believes it is highly unlikely that all of a firm's employees would have authority to read, write, and sign all of its electronic records.

83. One comment said authority checks are appropriate for document access but not system access, and suggested that the phrase "access the operation or device" be deleted. The comment added, with respect to authority checks on signing records, that in many organizations, more than one individual has the authority to sign documents required under FDA regulations and that such authority should be vested with the individual as designated by the operating organization. Another comment said proposed § 11.10(g) should explicitly require access authority checks and suggested that the phrase "use the system" be changed to "access and use the system." The comment also asked for clarification of the term "device."

The agency disagrees that authority checks should not be required for system access because, as discussed in comment 82 of this document, it is unlikely that a firm would permit any unauthorized individuals to access its computer systems. System access control is a basic security function because system integrity may be impeached even if the electronic records themselves are not directly accessed. For example, someone could access a system and change password requirements or otherwise override important security measures, enabling individuals to alter electronic records or read information that they were not authorized to see. The agency does not believe it necessary to add the qualifier "access and" because § 11.10(d) already requires that system access be limited to authorized individuals. The agency intends the word "device" to mean a computer system input or output device and has revised proposed § 11.10(g) to clarify this point.

Concerning signature authority, FDA advises that the requirement for authority checks in no way limits organizations in authorizing individuals to sign multiple records. Firms may use any appropriate mechanism to implement such checks. Organizations do not have to embed a list of authorized signers in every record to perform authority checks. For example, a record may be linked to an authority code that identifies the title or organizational unit of people who may sign the record. Thus, employees who have that corresponding code, or belong to that unit, would be able to sign the record. Another way to implement controls would be to link a list of authorized records to a given individual, so that the system would permit the individual to sign only records in that list.

84. Two comments addressed authority checks within the context of PDMA and suggested that such checks not be required for drug sample receipt records. The comments said that different individuals may be authorized to accept drug samples at a physician's office, and that the large number of physicians who would potentially qualify to receive samples would be too great to institute authority checks.

The agency advises that authority checks need not be automated and that in the context of PDMA such checks would be as valid for electronic records as they are for paper sample requests because only licensed practitioners or their designees may accept delivery of drug samples. The agency, therefore, acknowledges that many individuals may legally accept samples and, thus, have the authority to sign electronic receipts. However, authority checks for electronic receipts could nonetheless be performed by sample manufacturer representatives by using the same procedures as the representatives use for paper receipts. Accordingly, the agency disagrees with the comment that proposed § 11.10(g) should not apply to PDMA sample receipts.

The agency also advises that under PDMA, authority checks would be particularly important in the case of drug sample request records because only licensed practitioners may request drug samples.

Accordingly, proposed § 11.10(g) has been revised to read: "Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand."

85. Proposed § 11.10(h) states that procedures and controls for closed systems must include the use of device (e.g., terminal) location checks to determine, as appropriate, the validity of the source of data input or operational instruction. Several comments objected to this proposed requirement and suggested its deletion because it is: (1) Unnecessary (because the data source is always known by virtue of system design and validation); (2) problematic with respect to mobile devices, such as those connected by modem; (3) too much of a "how to;" (4) not explicit enough to tell firms what to do; (5) unnecessary in the case of PDMA; and (6) technically challenging. One comment stated that a device's identification, in addition to location, may be important and suggested that the proposed rule be revised to require device identification as well.

FDA advises that, by use of the term "as appropriate," it does not intend to require device checks in all cases. The agency believes that these checks are warranted where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized. In a network, for example, it may be necessary for security reasons to limit issuance of critical commands to only one authorized workstation. The device check would typically interrogate the source of the command to ensure that only the authorized workstation, and not some other device, was, in fact, issuing the command.

The same approach applies for remote sources connected by modem, to the extent that device identity interrogations could be made automatically regardless of where the portable devices were located. To clarify this concept, the agency has removed the word "location" from proposed § 11.10(h). Device checks would be necessary under PDMA when the source of commands or data is relevant to establishing authenticity, such as when licensed practitioners order drug samples directly from the manufacturer or authorized distributor without the intermediary of a sales representative. Device checks may also be useful to firms in documenting and identifying which sales representatives are transmitting drug sample requests from licensed practitioners.

FDA believes that, although validation may demonstrate that a given terminal or workstation is technically capable of sending information from one point to another, validation alone would not be expected to address whether or not such device is authorized to do so.

86. Proposed § 11.10(i) states that procedures and controls for closed systems must include confirmation that persons who develop, maintain, or use electronic record or signature systems have the education, training, and experience to perform their assigned tasks.

Several comments objected to the word "confirmation" because it is redundant with, or more restrictive than, existing regulations, and suggested alternate wording, such as "evidence." Two comments interpreted the proposed wording as requiring that checks of personnel qualifications be performed automatically by computer systems that perform database type

matches between functions and personnel training records.

The agency advises that, although there may be some overlap in proposed § 11.10(i) and other regulations regarding the need for personnel to be properly qualified for their duties, part 11 is specific to functions regarding electronic records, an issue that other regulations may or may not adequately address. Therefore, the agency is retaining the requirement.

The agency does not intend to require that the check of personnel qualifications be performed automatically by a computer system itself (although such automation is desirable). The agency has revised the introductory paragraph of § 11.10, as discussed in section VII. of this document, to clarify this point. The agency agrees that another word should be used in place of "confirmation," and for clarity has selected "determination."

87. One comment suggested that the word "training" be deleted because it has the same meaning as "education" and "experience," and objected to the implied requirement for records of employee training. Another comment argued that applying this provision to system developers was irrelevant so long as systems perform as required and have been appropriately validated. The comment suggested revising proposed § 11.10(i) to require employees to be trained only "as necessary." One comment, noting that training and experience are very important, suggested expanding proposed § 11.10(i) to require appropriate examination and certification of persons who perform certain high-risk, high-trust functions and tasks.

The agency regards this requirement as fundamental to the proper operation of a facility. Personnel entrusted with important functions must have sufficient training to do their jobs. In FDA's view, formal education (e.g., academic studies) and general industry experience would not necessarily prepare someone to begin specific, highly technical tasks at a given firm. Some degree of on-the-job training would be customary and expected. The agency believes that documentation of such training is also customary and not unreasonable.

The agency also disagrees with the assertion that personnel qualifications of system developers are irrelevant. The qualifications of personnel who develop systems are relevant to the expected performance of the systems they build and their ability to explain and support these systems. Validation does not lessen the need for personnel to have the education, training, and experience to do their jobs properly. Indeed, it is highly unlikely that poorly qualified developers would be capable of producing a system that could be validated. The agency advises that, although the intent of proposed § 11.10(i) is to address qualifications of those personnel who develop systems within an organization, rather than external "vendors" per se, it is nonetheless vital that vendor personnel are likewise qualified to do their work. The agency agrees that periodic examination or certification of personnel who perform certain critical tasks is desirable. However, the agency does not believe that at this time a specific requirement for such examination and certification is necessary.

88. Proposed § 11.10(j) states that procedures and controls for closed systems must include the establishment of, and adherence to, written policies that hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

Several comments suggested changing the word "liable" to "responsible" because the word "responsible" is broader, more widely understood by employees, more positive and inclusive of elements of honesty and trust, and more supportive of a broad range of disciplinary measures. One comment argued that the requirement would not deter record or signature falsification because employee honesty and integrity cannot be regulated.

The agency agrees because, although the words "responsible" and "liable" are generally synonymous, "responsible" is preferable because it is more positive and supportive of a broad range of disciplinary measures. There may be a general perception that electronic records and electronic signatures (particularly identification codes and passwords) are less significant and formal than traditional paper records and handwritten signatures. Individuals may therefore not fully equate the seriousness of electronic record falsification with paper record falsification. Employees need to understand the gravity and consequences of signature or record falsification. Although FDA agrees that employee honesty cannot be ensured by requiring it in a regulation, the presence of strong accountability and responsibility policies is necessary to ensure that employees understand the importance of maintaining the integrity of electronic records and signatures.

89. Several comments expressed concern regarding employee liability for actions taken under their electronic signatures in the event that such signatures are compromised, and requested "reasonable exceptions." The comments suggested revising proposed § 11.10(j) to hold people accountable only where there has been intentional falsification or corruption of electronic data.

The agency considers the compromise of electronic signatures to be a very serious matter, one that should precipitate an appropriate investigation into any causative weaknesses in an organization's security controls. The agency nonetheless recognizes that where such compromises occur through no fault or knowledge of individual employees, there would be reasonable limits on the extent to which disciplinary action would be taken. However, to maintain emphasis on the seriousness of such security breeches and deter the deliberate fabrication of "mistakes," the agency believes § 11.10 should not provide for exceptions that may lessen the import of such a fabrication.

90. One comment said the agency should consider the need for criminal law reform because current computer crime laws do not address signatures when unauthorized access or computer use is not an issue. Another comment argued that proposed § 11.10(j) should be expanded beyond "individual" accountability to include business entities.

The agency will consider the need for recommending legislative initiatives to address electronic signature falsification in light of the experience it gains with this regulation. The agency does not believe it necessary to address business entity accountability specifically in § 11.10 because the emphasis is on actions and accountability of individuals, and because individuals, rather than business entities, apply signatures.

91. One comment suggested that proposed § 11.10(j) should be deleted because it is unnecessary because individuals are presumably held accountable for actions taken under their authority, and because, in some organizations, individuals frequently delegate authority to sign their names.

As discussed in comments 88 to 90 of this document, the agency has concluded that this section is necessary. Furthermore it does not limit delegation of authority as described in the comment. However, where one individual signs his or her name on behalf of someone else, the signature applied should be that of the delegatee, with some notation of that fact, and not the name of the delegator. This is the