XIII. 전자 서명 – 확인 코드/패스워드 관리(Electronic Signatures--Controls for Identification Codes/Passwords)(Sec. 11.300)

The introductory paragraph of proposed Sec. 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.
섹션 11.300의 도입부에서는 패스워드와 조합된 확인 코드의 사용을 기반으로 하는 전자 서명은 그의 보안성과 완전성 보장을 위한 관리 대책을 구비해야 한다고 규정하고 있다.

To clarify the intent of this provision, the agency has added the words "[p]ersons who use" to the first sentence of Sec. 11.300. This change is consistent with Secs. 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: * * *."
이 조항의 의도를 명확히 하기 위하여, 섹션 11.300의 첫 문장에 "~를 사용하는 자는"을 추가했다. 이러한 변경은 섹션 11.10 및 11.30과도 일치한다. 이에 따라 도입부는 다음과 같이 변경되었다. "패스워드와 조합된 확인 코드의 사용을 기반으로 하는 전자 서명을 사용하는 자는, 보안성과 완전성 보장을 위해 다음을 포함하는 관리 대책을 구비해야 한다."

129. One comment suggested deletion of the phrase "in combination with passwords" from the first sentence of this section.
이 섹션의 첫 문장에서 "in combination with passwords"를 삭제하자는 의견이 1건 있었다.

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.
이 제안을 받아들일 수 없다. 그러한 변경은 ID 코드와 패스워드의 조합을 바탕으로 하는 전자 서명의 관리에 대한 원래 취지와 맞지 않으며, 실제로는 단일 컴포넌트로 구성된 비생체인식 기반의 전자 서명을 허용하는 결과로 이어질 수 있기 때문이다.

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

identification code and password.
섹션 11.300(a)는 ID 코드/패스워드의 관리에 ID 코드와 패스워드 발행 시의 고유성 유지가 포함되어야 한다고 규정하고 있다.

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.
대부분의 패스워드는 그 패스워드를 생성하는 사람에게 의미가 있는 일반적인 단어(예, 아이 이름, 주 이름, 도시 이름, 거리 이름, 달, 공휴일 또는 일자)라고 주장한 의견이 1건 있었다. 또한 ID 코드/패스워드 조합은 일반적으로 사용할 때마다 바뀌지 않으므로, 발행과 사용의 차이와 고유성의 의미에 대한 설명이 있어야 한다는 의견도 있었다.

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 Sec. 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.
전자 서명을 할 때마다 완전히 다른 ID 코드/패스워드를 사용하라는 것이 아니다. 16번 항목에서 설명한 이유로, 고유성이 필요한 것은 각각의 패스워드/ID 코드 조합이며, 이런 점을 명확히 하기 위하여 섹션 11.300(a)의 문구를 수정했다. 하지만 "호스트" 컴퓨터와 동조하여 연속으로 새로운 패스워드를 생성하는 확인 장치가 있음을 알고 있다. 이 장치를 사용하면, 시스템 접근을 할 때마다 고유한 패스워드가 생성될 것이다. 그러므로 이론적으로는 서명을 할 때마다 비생체인식성 전자 서명을 고유하게 생성할 수 있다.

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.
패스워드 생성자와 용이하게 연계시킬 수 있는 일반적인 단어로 된 패스워드의 사용은 주의가 필요하다. 그런 방식은 누군가가 패스워드를 추정하여 비보안(또는 심지어 다들

알고 있는) ID 코드와 조합해 다른 사람으로 가장하기가 상대적으로 용이하기 때문이다.

131. Proposed Sec. 11.300(b) states that controls for identification codes/passwords must ensure that code/password issuances are periodically checked, recalled, or revised.
섹션 11.300(b)는 ID 코드/패스워드 관리를 통해 확인 코드/패스워드 발행을 주기적으로 점검, 리콜 또는 수정해야 한다고 규정하고 있다.

Several comments objected to this proposed requirement because: (1) It is unnecessary, (2) it excessively prescribes "how to," (3) it duplicates the requirements in Sec. 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 Sec. 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.
이 기준에 대하여 이의를 제기한 의견이 다수 있었다. (1) 불필요하며 (2) "방법(how to)"을 과도하게 규정하고 있고 (3) 섹션 11.300(c)의 기준과 중복되며 (4) 큰 조직인 경우에는 관리가 불가능하기 때문이라는 이유에서다. 하지만 사람들이 주기적으로 패스워드를 변경하도록 해야 한다고 지적했다. 섹션 11.300(b)에 "패스워드 에이징 같은 이벤트" 등의 명확한 예를 포함시키자는 제안이 다수 있었다. 주기적 점검, 리콜, 수정을 누가 해야 하는지 규정해야 한다는 의견도 1건 있었다.

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 Sec. 11.300(c) because paragraph (c) specifically addresses followup to losses of electronic signature issuances, whereas Sec. 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.
반대 의견에 동의할 수 없다. 이 조항이 "how to"를 강조한다고 생각하지 않는다. 코드/패스워드 발행의 점검, 리콜, 수정 방법과 빈도를 결정하는데 있어서 충분한 유연성을 부여하고 있기 때문이다. 또한 섹션 11.300(c)는 전자 서명을 잃어버린 경우에 취할 사항을 다루고 있는 반면, 섹션 11.300(b)는 모르는 사이에 훼손되는 일이 없도록 하기

위하여 주기적인 변경이 필요함을 제시하고 있으므로, 이 둘이 중복된다고 생각하지 않는다. 사람들이 주기적으로 패스워드를 변경한다면, 이 기준을 충족하게 될 것이다.

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.
큰 조직에서는 이런 시스템 관리가 불필요하거나 불가능하다는 주장에도 동의할 수 없다. 사람이 많으면 ID 코드/패스워드가 훼손될 가능성도 증가하기 때문이다. 규모가 큰 조직이라면 주기적인 점검, 수정 또는 리콜 능력을 충분히 갖추어야 한다고 본다.

FDA agrees with the comments that suggested a clarifying example and has revised Sec. 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.
예를 포함시키자는 제안에 동의하여, 섹션 11.300(b)를 수정해 패스워드 에이징을 예로 제시했다. 하지만 이 예가 포함되었다고 해서, 패스워드 기간 만료만이 수정, 리콜, 점검의 유일한 근거가 된다는 의미로 해석해서는 안 된다. 예를 들어 ID 코드와 패스워드가 복사 또는 훼손되었다면 변경해야 한다.

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.
현재로써는 조직의 누가 이 시스템 관리를 수행해야 하는지 규정할 필요는 없다고 본다. 하지만 전자 서명을 발행한 부서가 이 일을 맡을 것으로 생각한다.

132. Proposed Sec. 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.
섹션 11.300(c)는 잃어버린 토큰, 카드 등의 권한을 전자적으로 해지하고 대리물의 적합하고 엄격한 관리를 통해 임시 또는 영구 교체물을 발행하는 분실 관리 절차를 ID 코드/패스워드 관리에 포함해야 한다고 규정하고 있다.

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.

이 섹션을 삭제해야 한다는 의견이 1건 있었다. "how to"를 과도하게 규정하고 있다는 이유에서다. 반면 이 규정은 충분히 자세하지 않다며 기본적인 카드 유형(예, magstripe, IC, optical)을 구분하고 각각에 대하여 별도의 섹션을 두어야 한다는 의견도 있었다. 다른 섹션과 달리 여기에서만 "엄격한 관리(rigorous controls)"를 요구하는 이유가 무엇인지 물은 의견이 2건 있었다. 잃어버리거나 도난 당한 카드 또는 장치에도 이 섹션을 적용해야 한다는 의견도 있었다.

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 Sec. 11.300(c) to replace "etc." with "and other devices that bear or generate identification code or password information."

분실 관리 절차를 구축하라는 기준이 너무 자세하거나 너무 일반적이라고 생각하지 않는다. 그런 절차의 세부 내용을 정하는데 있어서 충분한 유연성을 발휘할 수 있다. 현재로써는 다양한 유형의 카드나 토큰에 대하여 구체적인 기준을 제시할 필요는 없다고 생각한다. 그런 장치를 활용하는 조직도 충분한 유연성을 갖고 그의 운영에 대하여 적절한 관리 체계를 구축할 수 있다. ID 코드나 패스워드 정보를 포함하거나 생성하는 모든 종류의 장치를 대상으로 한다는 취지가 명확히 드러나도록 하기 위하여, "등(etc.)"을 "확인 코드 또는 패스워드 정보를 갖고 있거나 발생시키는 기타 장치"로 수정했다.

The agency agrees that Sec. 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.
섹션 11.300(c)는 장치가 훼손되는 방식에 상관없이 모든 분실 관리 절차를 대상으로 해야 한다는 의견에 동의하며, "lost" 다음에 "도난, 망실, 또는 훼손된 경우에"를 추가했다. 장치가 없어진 것은 오리지널 카드나 장치의 발행 및 관리가 적절하지 않은 결과일 수 있기 때문에, 그런 문제의 재발을 방지하기 위해서는 보다 엄격한 대책이 필요하다는 생각에서 "rigorous"라는 표현을 사용했다. 예를 들어 장치의 안전한 관리에 대한 작업자 훈련을 강화할 필요가 있을 수 있다.

133. Proposed Sec. 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.
섹션 11.300(d)는 패스워드 및/또는 ID 코드의 무허가 사용을 방지하고, 무허가 사용 시도를 긴급한 방식으로 감지하여 시스템 보안 조직과 경영자에게 보고하는 트랜잭션 보안 장치의 활용이 ID 코드/패스워드 관리에 포함되어야 한다고 규정하고 있다.

Several comments suggested that the term "emergent" in proposed Sec. 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.
(1) 적시 보고면 충분할 수 있고, (2) 긴급하게 보고하는 기술이 없으며, (3) 적시라는 표현이 보다 인식 가능하며 일반적인 표현이라는 이유에서, ID 코드/패스워드의 무허가 사용 시도와 관련한 보고에서 "긴급한(emergent)"을 "적시에(timely)"로 교체하자는 의견이 다수 있었다.

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.
이 의견에 부분적으로 동의한다. ID 코드 및 패스워드의 무허가 사용 시도는 전자 서명 및 전자 기록서 변조, 데이터 부정 행위, 또는 심한 경우에는 궁극적으로 많은 비용을 발생시킬 수 있는 결과의 징조일 수 있으므로, 그런 시도는 매우 심각한 것이라고 생각한다. 그와 같은 시도가 있다면, 화재 경보에 대응하는 것과 동일한 방식으로 적절한 보안 담당자에게 즉각적이고 긴급하게 알려줄 필요가 있다고 생각한다. 이런 취지를 보다 이해하기 쉬운 표현으로 명확히 하기 위하여, "emergent"를 "즉각적이고 긴급한(immediate and urgent)"으로 바꿨다. ID 코드 및 패스워드를 수용/기각하는 것과 같은 기술을 활용해 오용 시도와 관련한 메시지를 보안 담당자에게 전달할 수 있다고 본다.

134. One comment suggested that the word "any" be deleted from the phrase "any attempts" in proposed Sec. 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.
섹션 11.300(d)의 "any attempts"에서 "any"를 삭제하자는 의견이 1건 있었다. 너무 과도한 표현이라는 이유에서다. 또한 허가 받지 않은 사람이 시스템에 들어가거나 파일에 접근하려는 시도는 매우 심각한 것이라고 지적하며, "any" 대신에 "all"을 쓰자는 의견도 있었다. 허가 받지 않은 사람이 개인 ID 코드와 패스워드를 찾아내는데 사용할 수 있는 장치가 시중에 나와 있다고 덧붙였다.

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.
ID 코드와 패스워드의 오용 시도 모두를 포괄하는데 "any"라는 표현이 적절하다고 생각하며, 이를 삭제하자는 의견을 거부한다. "any"를 삭제한다면, 기본적으로 외부인이 침투할 수 있는 철저하지 않은 시스템에서는 탄로날 가능성이 적다고 생각할 수 있다. 위의

의견에서 언급한 "스니핑" 장치에 대해 알고 있으며, 이에 대항하여 적합한 대응책을 마련할 필요가 있다고 본다.

135. One comment suggested that proposed Sec. 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.
섹션 11.300(d)는 특히 단순한 타이핑 오류 시에는 현실성이 없으므로 삭제해야 한다는 의견이 1건 있었다. 또한 시스템에 접근할 때 단순히 잘못된 키를 누를 수 있다는 이유에서, 이 섹션은 시스템이 아니라 전자 기록서에 대한 접근과 관련된 것이어야 한다는 의견도 있었다.

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.
133번과 134번 항목에서 설명한 바와 같이, 이 조항은 필요하고 합리적인 것이라고 생각한다. 보안 관련 부분은 기록서 접근뿐만 아니라 시스템 접근까지 포함한다. 일단 허가를 받지 않고 시스템에 접근하고 나면, 패스워드를 바꿔 추가적인 침입과 부정 행위를 은폐할 수 있다. 이 섹션을 삭제하면 변조 확률이 더 높아지며 보안 담당자가 알지도 못할 수 있다.

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.
하지만 단순한 타이핑 오류는 무허가 사용 시도를 의미하지 않을 수 있지만, 단기간에 연속하여 그런 오류가 나타나거나 그 ID 코드나 패스워드를 "소유"한 사람이 없거나 부재중이거나 접속 시도를 할 수 없는 것으로 알려진 경우에 그런 오류가 발생한다면, 이는 심각한 보안 문제의 신호일 수 있고 이를 무시해서는 안 된다. 무허가 사용 시도의 유형 결정에 있어서 이 섹션은 최대한의 자율권을 부여하고 있다.

136. One comment suggested substituting the phrase "electronic signature" for "passwords and/or identification codes."
"패스워드 및/또는 ID 코드" 대신에 "전자 서명"을 사용하자는 의견이 1건 있었다.

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.
이 의견에 동의하지 않는다. 이런 식으로 수정하면 전자 서명을 구성하는 중요 요소의 오용 시도(예, "패스워드" 공격)를 무시하는 결과가 발생할 수 있기 때문이다.

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.
(1) 오용 시도를 해당 보안 부서에 보고하면서 동시에 경영자에게 보고하는 것은 필요하지 않고, (2) 보안 조직은 자체 절차와 보고 라인을 통해 경영자에게 보고하며, (3) 경영자가 항상 관여하지 않을 수 있다는 주장이 다수 있었다.

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 Sec. 11.300(d) to give organizations maximum flexibility in establishing criteria for management notification. Accordingly, Sec. 11.300(d) now states that controls for identification codes/passwords must include:
보안 조직이 상황을 파악하고 적절하게 대응한다면, 모든 오용 시도를 동시에 경영자에게 보고할 필요가 없다는 점에 동의한다. 하지만 경영자에게 즉각적이고 긴급하게 알려야 할 정도로 충분히 심각한 보안 위반 행위가 일부 있을 수 있다. 그에 따라 경영자 통보 기준의 설정과 관련하여 최대한의 유연성을 부여하는 식으로 섹션 11.300(d)를 수정했다. 이제 섹션 11.300(d)는 다음 사항이 확인 코드/패스워드 관리에 포함되어야 한다고 규정하고 있다.

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.
패스워드 및/또는 확인 코드의 무허가 사용을 방지하고 무허가 사용 시도를 즉각적이고 긴급한 방식으로 감지하여 시스템 보안 조직과 적절한 경우에는 경영진에게 보고하는 트랜잭션 보안 대책을 구비하여 활용한다.

138. Proposed Sec. 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.
섹션 11.300(e)는 식별 정보를 갖고 있는 토큰 또는 카드 같은 장치를 처음 도입할 때는 적절하게 기능을 수행하는지 테스트하고 이후 주기적으로 테스트해야 한다는 점이 ID 카드/패스워드 관리에 포함되어야 한다고 규정하고 있다.

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 Sec. 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.
이 장치 테스트 기준이 불필요하다며 반대한 의견이 많았다. 이 테스트는 시스템 밸리데이션의 일부이며, 작동하지 않는 장치는 시스템 접근을 허용하기보다는 거부한다는 점에서 이런 장치는 접근 문제가 없다고 주장했다. 문제가 있는 장치는 사용자 접근을 거부해야 한다는 식으로 이 섹션을 수정하자고 제안했다. "식별 정보"의 의미가 명확하지 않고, 카드가 일종의 토큰이기 때문에 "토큰 또는 카드"는 중복되는 표현이라고 지적한 의견도 1건 있었다.

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.
이 기준을 포함시킨 이유를 명확히 제시하고, 시스템 접근 이외에 식별 정보와 보안 성능 특성 요소의 정확성이 장치 기능에 포함됨을 강조하고자 한다. 시스템 접근성 테스트만으로는 허가 받지 않은 장치 변형을 파악할 수 없다. 예를 들어 어떤 장치가 변형되어 식별 정보가 바뀌었다면, 시스템 접근이 허용될 수 있고, 그에 따라 누군가가 다른 사람처럼 행동할 수 있다. 또한 조직이 부여한 것 이상의 추가적인 시스템 권한과 행위 허가를 부여하는 식으로 장치가 변경될 수도 있다. 중요성이 덜하기는 하지만 그런 장치의 단순한 손상이 발생해 기능이 제대로 수행되지 못하기도 한다. 예를 들어 바코드가 손상되거나 오염되거나 기타 다른 방식으로 알아볼 수 없게 되면, 의도했던 바의 일관된 정확성을 갖고 바코드를 읽을 수 없게 된다. 접근이 허용되기는 하겠지만, 예상 이상의 많은 스캐닝을 거쳐야 할 것이다. 장치 테스트는 그런 결함을 찾아내기 위한 것이다.

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.
전자 서명 시스템의 밸리데이션은 허가 받지 않은 장치 변형이나 이후의 손상을 포괄하지 않으므로, 밸리데이션을 한다고 해서 주기적인 테스트의 필요성이 없어지지는 않는다.

The agency notes that Sec. 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 Sec. 11.300(e) to clarify the agency's intent and to be consistent with Sec. 11.300(c). Revised Sec. 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.
섹션 11.300(e)는 활용 가능한 장치의 유형을 제한하고 있지 않다. 또한 모든 토큰이 카드는 아니며, 식별 정보는 ID 코드와 패스워드를 포함한다. 그러므로 원래의 취지를 명확히 하고 섹션 11.300(c)와 일관성을 갖도록 섹션 11.300(e)를 다음과 같이 수정했다. "확인 코드 또는 패스워드 정보를 갖고 있거나 발생시키는, 토큰이나 카드 같은 장치를 처음 도입할 때 테스트하고 이후 주기적으로 테스트하여, 적절하게 기능을 발휘하며 허가

받지 않은 방식으로 변형되지 않았음을 확인한다."