CROMERR System Checklist

Item	Checklist Item	Citation	Regulatory Language
18b	Inclusion of electronic signatures	3.3 definition of copy of record	See item 8 for definition of copy of record.
Preamble Language: "The method of inclusion may vary, depending on the nature of the signature. With a digital signature, created by encrypting a hash of the document being signed with the private key in a private/public key-pair, the signature is simply a number that can and should be contained as a copy of record element. There is no risk of signature theft in this case. Each digital signature is bound to the specific document it signs, and the private key, which is actually used for signing, is inaccessible to a would-be intruder. With other forms of signature such as personal identification numbers (PINs) or passwords, items of personal information, or biometric images or values, including the signature as a copy of record element may raise signature theft issues. At least in theory, such signatures could be detached or copied from a copy of record and re-used spuriously without detection. To address this risk, the signature, especially in the case of a PIN or password, may be encrypted for storage, perhaps together with a hash of the document signed, to bind the signature to the document content. Another approach may be to validate the signatory's identity, e.g. by comparing a signatory-generated password with an encrypted version maintained securely at the electronic document receiving system. In such cases, the signatory-generated password – which might be regarded as the signature – never actually appears on the electronic document, so the signature that is "included" in the copy of record may be an encrypted form of the signature, or possibly nothing exactly corresponding to a signature at all, but rather pointers or references to the processes or encrypted data that provide the actual link to the signatory. There are analogous strategies for biometric signatures. For example, the validity of a biometric (e.g., a finger print, a retinal scan, etc.) may be established by using certain statistical algorithms to evaluate data provided by the biometric. In such cases, the copy of record might document the process of validating the signature, but without including the biometric data that was used to show that the signature was valid. On any of these approaches, the copy of record may satisfy the requirement that the copy "include" the signatures, provided that what the copy does contain serves to establish whether the electronic document			
18c	Inclusion of date and time of receipt	3.3 definition of copy of record	See item 8 for definition of copy of record.
Preamble Language: "This is not generally problematic, except in cases of continuous streams of data conveyed to the system. For such continuous data, reasonable alternatives may be substituted that serve the same purposes, for example, associating stages of the data flow with dates and times, say, at hourly intervals."			
18d	Inclusion of other information necessary to record meaning of document	3.3 definition of copy of record	See item 8 for definition of copy of record.
Preamble Language: "Similarly, the copy of record may include other additional information to the extent that this is needed to establish the meaning of the content and the circumstances of receipt. Such additional information might include data field labels, signatory information such as references to PKI certificates, and transmission source information."			
18e	Ability to be viewed in human-readable format	3.3 definition of copy of record	See item 8 for definition of copy of record.
Preamble Language: "The copy of record may satisfy this requirement in many different ways. It might actually include explicit labels or descriptions for each data element or information item, or preserve a visual format in which the data were submitted. Alternatively, it may incorporate a conventional ordering of the items or elements, where the information that associates such ordered data with labels, descriptions, or other means of visual display is maintained externally and can be invoked as needed – for example, to make the data elements appear within fields in the image of a filled-out form. Where the electronic document is created off-line by the submitter and conveyed as a whole to the receiving system, it is preferable for the copy of record to reflect the mechanism or format for indicating meaning supplied in the submission. For example, if the submission is in some standard electronic data interchange format, then the copy of record might usefully preserve that format. Taking this approach will help to resolve potential chain of custody issues if questions arise about whether the copy of record is true and correct. However, in cases where the electronic document is created on-line, for example, through the use of a web-form, the format for the copy of record will of necessity be an artifact of the electronic document receiving system itself. This is not problematic, as long as the system provides a way to ensure that the meaning of each data element as supplied by the submitter remains unambiguous....The requirement does not mean that the data must be stored in a human-readable format, so long as there is a well-documented way to display the stored data in such a format."			
19	Timely availability of copy of record as needed	3.2000(b)(1) - (2) and 3.3 definition of *copy of record*	Same as item 18.
Preamble Language: Section 3.2000(b) reflects the role that electronic document receiving systems play in supporting a wide range of compliance and enforcement-related activities, including compliance research and analysis, civil actions, and litigation, and the fact that the success of such activities may be affected by the relative ease or difficulty of accessing the data related to electronic submissions. Accordingly, electronic document receiving systems must provide timely access to such data, especially to data relevant to the questions of what was submitted, by whom, and, where signatures are involved, who the signatories were and to what they certified. Much of this data may be assembled in the copy of record, together with any data needed to establish that the copy is a "true and correct copy of an electronic document received," as specified by the section 3.3 *copy of record* definition. To help the litigator develop evidence and present it in the courtroom, it is advisable that the copy of record be maintained and made accessible in a form and format that requires the minimum possible "assembly" of its elements, so that its connection with what was received and what was certified to by any signatories is easy to understand and to demonstrate to others."			
20	Maintenance of copy of record	3.2000(b)(1) - (2) and 3.3 definition of *copy of record*	Same as item 18.