LESSON 6: USING THE CHECKLIST TO WORK THROUGH SYSTEM REQUIREMENTS

Lesson 5 described how CROMERR presents the system requirements for receiving electronic reports, with a focus on the system- and enforcement-related requirements.

Lesson 6 describes how these same requirements are presented in the CROMERR System Checklist (which was introduced in Lesson 4). You may want to refer to the checklist as you step through this lesson.

The CROMERR System Checklist describes the CROMERR system requirements as they affect the following five system processes:

1. Registration;
2. Signature Process;
3. Submission Process;
4. Signature Validation; and
5. COR.

This lesson covers these five processes in detail, and:

- Shows how the CROMERR requirements and checklist processes are interrelated; and
- Suggests how to use the CROMERR System Checklist Template in conjunction with the CROMERR System Checklist to describe how your system meets the CROMERR system requirements.

Note: The CROMERR System Checklist is not a required part of your CROMERR application; instead, it is a tool created to assist you as you work toward meeting the requirements.

Processes three and five are involved in electronic submissions, while processes one, two, and four are only involved where the submissions include an electronic signature.

REGISTRATION

Checklist items 1 through 4 are grouped under the Registration Process, where users establish their accounts in the system. This process typically requires users to provide information about them. The system administrator then reviews this information and provides the users with system privileges and signing credentials. Checklist items 1 through 4 represent CROMERR requirements that this registration process must satisfy.

1. Identity-Proofing of Registrant—For users who will sign electronic reports, CROMERR requires that the system determine the individual's identity, usually as a part of the registration process.

This identity-proofing is the one CROMERR requirement that is more stringent for users who will sign Priority Reports.

For users who will sign Priority Reports, CROMERR requires that the system establish their identity before accepting reports with their electronic signatures. There are two ways to do this. One is to establish identity through verification by, and attestation of, a disinterested party, based on identifiers—at least one of which is government-issued. The other way is to include the registrant's handwritten signature as part of the electronic signature agreement (ESA) process. Where the ESA is executed on paper with a handwritten signature, it is called a "subscriber agreement."

For users who sign only Non-Priority Reports, CROMERR does not specify when or how the identity proofing must be done, although either method specified for Priority Reports will satisfy the requirement in the non-priority case.

Reference: CROMERR § 3.2000(b)(5)(vii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

(vii) For each electronic signature device used to create an electronic signature on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; or

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; or

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

A **disinterested individual** is an individual who is not connected with the person in whose name the electronic signature device is issued. A disinterested individual is not any of the following: The person's employer or employer's corporate parent, subsidiary, or affiliate; the person's contracting agent; member of the person's household; or relative with whom the person has a personal relationship.

A **subscriber agreement** is an electronic signature agreement signed by an individual with a handwritten signature. This agreement must be stored until five years after the associated electronic signature device has been deactivated.

A **local registration authority** is an individual who is authorized by a state, tribe, or local government to issue an agreement collection certification, whose identity has been established by notarized affidavit, and who is authorized in writing by a regulated entity to issue agreement collection certifications on its behalf.

An **agreement collection certification** is a signed statement by which a local registration authority certifies that a subscriber agreement has been received from a registrant; the agreement has been stored in a manner that prevents unauthorized access to these agreements by anyone other than the local registration authority; and the local registration authority has no basis to believe that any of the collected agreements have been tampered with or prematurely destroyed.

2. **Determination of Registrant's Authority—**CROMERR requires the system to determine that users who will sign reports are actually authorized to do so on behalf of the specified regulated entities. This determination is usually based on some combination of the program's existing knowledge of the regulated entities, information submitted by the users or officials of the regulated entities, and some follow-up verification—such as phone calls or as a part of routine inspections.

Reference: § 3.2000(b)(5)(vii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

(vii) For each electronic signature device used to create an electronic signature on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; **OR**

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; **OR**

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

3. **Issuance (or Registration) of a Signing Credential in a Way that Protects it from Compromise—** CROMERR requires the system to provide users who will sign electronic reports with electronic signature devices (or credentials) to execute their electronic signatures. These devices could be passwords, PINs, PKI certificates associated with private-public key pairs, physical tokens such as a USB device, or devices incorporating biometrics (e.g., fingerprints). Whatever device is issued (or registered), there are two basic requirements that need to be met. The first is to ensure that a device intended for a specific, identified user is issued only to that individual. The second is to ensure that the process of issuing that device—and maintaining a record of it on the system—protects the device from compromise.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing"

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she

must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

4. **Electronic Signature Agreement**—CROMERR requires that users sign an Electronic Signature Agreement, and this is normally part of the registration process. This agreement must include language that obligates the registrant to protect the credential from compromise, and to immediately report any evidence of compromise to the system administrator. The agreement must also include a statement that the registrant understands that any electronic signature executed with the electronic signature device is as legally binding as a handwritten signature.

   Reference: § 3.2000(b)(5)(v)

   "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

   (v) Each signatory has signed either an electronic signature agreement or a subscriber agreement with respect to the electronic signature device used to create his or her electronic signature on the electronic document."

   An **electronic signature agreement** is an agreement signed by an individual with respect to an electronic signature device that the individual will use to create his or her electronic signatures requiring such individual to protect the electronic signature device from compromise; to promptly report to the agency... or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised; and to be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature.

   A **subscriber agreement** is an electronic signature agreement signed by an individual with a handwritten signature. This agreement must be stored until five years after the associated electronic signature device has been deactivated.

Signature Process

Checklist items 5 through 7 are grouped under the Signature Process and represent CROMERR requirements that this process must satisfy.

5. **Binding of Signatures to Document Content**—CROMERR requires that all electronic signatures be bound to the document content. This means that the system must provide a way to ensure that the document content is, in effect, "locked" so that it cannot be subject to undetectable changes once the signature is executed.

Reference: § 3.2000(b)(5)(ii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(ii) The electronic document cannot be altered without detection at any time after being signed."

6. **Opportunity to Review Document Content—**CROMERR also requires that the signature process provide the signers with the opportunity to review the content of the document they are signing.

Reference: § 3.2000(b)(5)(iii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(iii) Each signatory had the opportunity to review in a human-readable format the content of the electronic document that he or she was certifying to, attesting to or agreeing to by signing."

7. **Opportunity to Review Certification Statements and Warnings**—Along with the opportunity to review document content, CROMERR also requires that signers have the opportunity to review certification statements—including any applicable warnings of criminal penalties for false certifications—before asking them to execute their electronic signatures.

Reference: § 3.2000(b)(5)(iv)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(iv) Each signatory had the opportunity, at the time of signing, to review the content or meaning of the required certification statement, including any applicable provisions that false certification carries criminal penalties."

Submission Process

Checklist items 8 through 12 are grouped under the Submission Process, and represent the CROMERR requirements that must be satisfied as the report or document is transferred to the system during a formal submission. Items 8 through 11 are required for all submittals, whether or not an electronic signature is included.

8. **Transmission Error Checking and Documentation**—CROMERR requires that the system be able to assure that it received the electronic report through an error-free transmission or that any errors in transmission are documented. This normally involves the use of cryptographic technologies (e.g., secure socket layer).

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

9. **Opportunity to Review COR**—CROMERR requires that the system provide the submitter and any signers with the opportunity to review the Copy of Record (COR) of the submittal after it is formally received. This is distinct from the requirement that signers have the opportunity to review document content and certification statements prior to signing and submitting, which are addressed in items 6 and 7. The requirement here has three elements. First, the system must

notify the submitter and any signers that the COR is available for their review. Second, the system must produce a version of the COR in a human-readable format. Third, and finally, the system must provide the signers and submitter with access to the COR in this human-readable format.

Reference: § 3.2000(b)(4)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(4) Any individual identified in the electronic document submission as a submitter or signatory had the opportunity to review the copy of record in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information and had the opportunity to repudiate the electronic document based on this review."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

10. Procedures to Address Repudiation COR—CROMERR requires that the submitter and any signers have the opportunity to repudiate the Copy of Record (COR) in part or in total, if they disagree with how the COR represents the submission. The system must also have a way to address any cases of repudiation and to document the history of the submission in those cases.

Reference: § 3.2000(b)(1)–(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

11. Procedure to Flag Accidental Submissions—CROMERR requires that the system be able to identify accidental or counterfeit submissions and have a way of addressing user repudiations of submissions as forged or accidental. For those cases, the system must also be able to document the submission's history.

Reference: § 3.2000(b)(3)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(3) The electronic document was submitted knowingly and not by accident."

12. Automatic Acknowledgement of Submission—Where the submission includes an electronic signature, CROMERR requires that the system automatically send an acknowledgement to the individual identified as the signer at the time of submittal. The acknowledgement must identify the submittal, the signers, and the date and time the submittal was received.

This automatic acknowledgement must be sent to an "out-of-band" address—that is, an address that does not share the same access controls like the username, PIN, or password—as the account used to make the electronic submission. This address is typically an email address, but it could be a U.S. Postal address or even a phone number.

One purpose of this requirement is to help system users detect any compromise of their signature devices. If a submission includes a signature executed with a device by someone other than its registered owner, the owner will be alerted by the acknowledgement he or she receives at the out-of-band address. Given this purpose, the system must include procedures to follow-up when the acknowledgement cannot be delivered to determine whether the email or U.S. Postal address associated with the account is still valid.

Reference: § 3.2000(b)(5)(vi)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to

generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(vi) The electronic document receiving system has automatically responded to the receipt of the electronic document with an acknowledgment that identifies the electronic document received, including the signatory and the date and time of receipt, and is sent to at least one address that does not share the same access controls as the account used to make the electronic submission."

Signature Validation

Checklist items 13 through 17 are grouped under the Signature Validation Process, and represent CROMERR requirements that the system must satisfy as part of ensuring that electronic signatures it receives are valid.

13. Credential Validation—For each electronic signature received, CROMERR requires that the system verify that the identified signer is actually authorized to sign the submittal.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she

must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

14. **Signatory Authorization**—Under the Submission Process, CROMERR requires that the system be able to flag counterfeit submittals. Under the Signature Validation Process, CROMERR also requires that the system be able to flag counterfeit credential use, which would indicate that the credential has been compromised.

    Reference: § 3.2000(b)(5)(i)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

    (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

    (i) Each electronic signature was a valid electronic signature at the time of signing."

    A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

    An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

15. **Procedures to Flag Counterfeit Credential Use**—CROMERR requires that the system include procedures to follow up on evidence and reports of credential compromise, including procedures to revoke a credential when compromise is indicated. Correspondingly, the system must be able to reject submissions that include e-signatures executed with revoked credentials.

    Reference: § 3.2000(b)(5)(i)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner,

including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

16. Procedures to Revoke or Reject Compromised Credentials—CROMERR requires that the system include procedures to follow up on evidence and reports of credential compromise, including procedures to revoke a credential when compromise is indicated. Correspondingly, the system must be able to reject submissions that include e-signatures executed with revoked credentials.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

17. **Confirmation of Signature Bindings to Document Content**—Related to item 5—requiring signature binding—CROMERR requires that the system be able to determine whether the content of an electronically-signed submittal matches the content at the time the signature was executed.

Reference: § 3.2000(b)(5)(ii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(ii) The electronic document cannot be altered without detection at any time after being signed."

Copy of Record (COR)

Checklist items 18 through 20 are grouped under the fifth and final process, the COR Process. These items represent CROMERR requirements that the system must satisfy in creating and maintaining CORs. The items address:

- What data CORs must capture;
- How access to CORs must be provided to program and enforcement staff; and
- How the CORs must be maintained.

18. **Creation of COR**—§ 3.2000(b)(1) through (2): For each legitimate submittal received, CROMERR requires the system to create a COR. The COR must be a "true and correct copy" of the submittal, in the sense that it must have exactly the same informational content as the submittal; otherwise, it must document any changes to this content after submittal.

The COR must include all associated signatures, the date and time of receipt, and any other information necessary to interpret the submittal.

Finally, the COR must be viewable in a human-readable format that makes the meaning of each information item clear; although it need not be maintained in this format or in the format in which the submittal was originally received.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

19. Timely Availability of COR, as needed—§ 3.2000(b)(1) through (2): CROMERR requires the system to provide program and enforcement staff with timely access to the CORs and the associated documentation.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures

contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

20. Maintenance of COR—CROMERR requires the system to maintain the CORs for as long as needed by program or enforcement staff. The CORs must be maintained together with any information needed to document their integrity, such as records or logs of associated signature validation processes. Finally, the CORs must be maintained in a way that protects them from alteration or deletion on a system that is electronically and physically secure.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

The CROMERR Requirements and the Checklist Items

From the detailed discussion of the CROMERR System Checklist items, it should be evident that each checklist item corresponds to specific CROMERR requirements, and vice versa.

The tables on the next two pages make this correspondence explicit.

- The first table maps CROMERR requirements to the corresponding checklist items.
- The second table maps checklist items to the corresponding CROMERR requirements.

The CROMERR Requirements and the Related Checklist Items

System Requirements	Related Checklist Items
§ 3.2000(b)(1): The e-document is not alterable without detection.	Items 8, 10, 18
§ 3.2000(b)(2): Alterations to the e-document are documented by the system.	Items 8, 10, 18
§ 3.2000(b)(3): The e-document can only be submitted intentionally.	Item 11
§ 3.2000(b)(4): Submitters and signers can review the COR of the e-document.	Item 9
§ 3.2000(b)(5): If an e-signature is required, then the e-document meets e-signature requirements:	
(i) Signature valid at time of signing	Items 1, 2, 3, 13, 14, 15, 16
(ii) Document cannot be altered without detection after signing	Items 5, 17
(iii) Opportunity to review content	Item 6
(iv) Opportunity to review certifications statement	Item 7
(v) Receipt Acknowledgement	Item 4
(vi) E-signature agreements	Item 12
(vii) Identity proofing with legal certainty	Items 1, 2

Mapping Processes and Checklist Items to Requirements

Checklist Items	System Requirement
Registration	
1. Identity-Proofing of Registrant	§ 3.2000(b)(5)(vii)
2. Determination of Registrants Signing Authority	§ 3.2000(b)(5)(vii) § 3.2000(b)(5)(i)
3. Issuance (or Registration) of a Signing Credential in a Way that Protects it from Compromise	§ 3.2000(b)(5)(i)
4. Electronic Signature Agreement	§ 3.2000(b)(5)(v)
Signature Process	
5. Binding of Signatures to Document Content	§ 3.2000(b)(5)(ii)
6. Opportunity to Review Document Content	§ 3.2000(b)(5)(iii)
7. Opportunity to Review Certification Statements and Warnings	§ 3.2000(b)(5)(iv)
Submission Process	
8. Transmission Error Checking and Documentation	§ 3.2000(b)(1)(2)
9. Opportunity to Review COR	§ 3.2000(b)(4)
10. Procedures to Address Submitter or Signatory	§ 3.2000(b)(1)(2)
11. Procedure to Flag Accidental Submissions	§ 3.2000(b)(3)
12. Automatic Acknowledgement of Submission	§ 3.2000(b)(5)(vi)
Signature Validation	
13. Credential Validation	§ 3.2000(b)(5)(i)
14. Signatory Authorization	§ 3.2000(b)(5)(i)
15. Procedures to Flag Counterfeit Credential Use	§ 3.2000(b)(5)(i)

Checklist Items	**System Requirement**
16. Procedures to Revoke or Reject Compromised Credentials	§ 3.2000(b)(5)(i)
17. Confirmation of Signature Binding to Document Content	§ 3.2000(b)(5)(ii)
COR	
18. Creation of COR	§ 3.2000(b)(1)(2)
19. Timely Availability of COR, as needed	§ 3.2000(b)(1)(2)
20. Maintenance of COR	§ 3.2000(b)(1)(2)

THE CROMERR SYSTEM CHECKLIST AND THE SYSTEM CHECKLIST TEMPLATE

The CROMERR System Checklist can help states that are preparing their CROMERR applications in two ways:

- First, it explains the CROMERR system requirements as specific system processes.
- Second, it provides an approach for documenting how a system meets CROMERR requirements, by describing how the system provides for each of the Roadmap items.

To support the second use of the checklist, EPA has also developed a corresponding CROMERR System Checklist Template—a document that provides a format for describing how the states system satisfies each of the checklist items. **While the CROMERR System Template is not required for application, EPA strongly recommends its use.**

For each checklist item, the template provides three blank spaces, for:

- Business Practices
- System Functions
- Supporting Documentation (a list of attachments)

Depending on the systems solution for the item, the description may fit into one, two, or all of these blanks.
The CROMERR Web site, at http://www.epa.gov/cromerr, provides several examples of how to use the CROMERR System Checklist Template to successfully document CROMERR-compliant systems for receiving electronic reports.