**CROMERR Reviewer Guide**

**May 1, 2017**

This document is a tool used by EPA to assist in reviewing CROMERR applications that include a CROMERR checklist. It contains an overview of the CROMERR checklist, which provides a general description of CROMERR requirements and definitions of key terms as defined in the CROMERR rule. It also includes a detailed description of each item of the CROMERR application checklist, and provides the questions used by EPA to evaluate CROMERR checklists.

This document includes internal links to facilitate navigation. Blue underlined text indicates internal links that redirect users to the selected section. The Checklist Overview below serves as a table of contents, with links to the specific CROMERR checklist items. Click each CROMERR checklist item to go to the CROMERR Reviewer Guide section for that item. Click on italicized words to go to a description of a general CROMERR topic or the CROMERR definition for that word. Depending on your settings, you may need to CTRL-click to activate the links.

|  |  |  |  |
| --- | --- | --- | --- |
| **Checklist Overview** | | | |
| The CROMERR checklist describes the business practices and system functions an applicant will use to satisfy section 3.2000(b) requirements for electronic document receiving systems. The 3.2000(b) requirements cover practices/functions for:   1. [*Registration*](#Reg) – establishing user accounts and electronic signature (e-signature) credentials, and executing an electronic signature agreement;  * [Item 1: Identity-proofing of registrant](#Item1) * [Item 2: Determination of registrant's signing authority](#Item2) * [Item 3: Issuance (or registration) of a signing credential in a way that protects it from compromise](#Item3) * [Item 4: Electronic signature agreement](#Item4)  1. [*Signature* *Process*](#SigProc)– providing for secure signature/certification of electronic documents (e-documents) that assures their non-repudiation;  * [Item 5: Binding of signatures to document content](#Item5) * [Item 6: Opportunity to review document content](#Item6) * [Item 7: Opportunity to review certification statements and warnings](#Item7)  1. [*Submission* *Process*](#SubProc)– providing for secure submission of e-documents that assures their integrity;  * [Item 7: Opportunity to review certification statements and warnings](#Item7) * [Item 8: Transmission error checking and documentation](#Item8) * [Item 9: Opportunity to review copy of record](#Item9) * [Item 10: Procedures to address submitter/signatory repudiation of a copy of record](#Item10) * [Item 11: Procedures to flag accidental submissions](#Item11) * [Item 12: (e-signature cases only) Automatic acknowledgment of submission](#Item12)  1. [*Signature Validation*](#SigVal) – determining that the system has received valid electronic signatures, that is, e-signatures created with electronic signature devices that are not compromised and belong to the authorized signatories;  * [Item 13: Credential Validation](#Item13) * [Item 14: Signatory authorization](#Item14) * [Item 15: Procedures to flag spurious credential use](#Item15) * [Item 16: Procedures to revoke/reject compromised credentials](#Item16) * [Item 17: Confirmation of signature binding to document content](#Item17)  1. [*Copy of Record (COR*](#COR)*)* – creating and maintaining authoritative official copies of electronic submissions that meet legal requirements.  * [Item 18. Creation of copy of record](#Item18) * [Item 19. Timely availability of copy of record as needed](#Item19) * [Item 20. Maintenance of copy of record](#Item20)   **General Requirements**  In one way or another, the Checklist items are all aimed at ensuring that the e-documents a system receives and maintains are what the submitter intended to submit and that the e-document content is what any individuals named as signers intended to certify as true or accurate. To meet this general requirement, the Checklist, and CROMERR itself, focuses on **three general themes**: COR integrity; uncompromised e-signature devices; and submitter/signer access to what was submitted/signed.  **COR integrity:** As the official copy of the submission, the COR must be created as a “true and correct” copy of submission’s content, and must be maintained in a way that preserves its truth and correctness for as long as it is retained. The Checklist addresses these requirements in:   * Item 5 –   + (5G) the content of the COR;   + (5H – 5K) ensuring that the COR cannot be tampered with; * Item 9 – providing the submitter and any signer the opportunity to review the COR once it is created; * Item 10 –   + (10E – 10J) correcting a COR and documenting the corrections;   + (10K – 10L) maintaining a repudiated COR or disposing of it; * Item 11 –   + (11C) determining whether a COR reflects an accidental submission;   + (11F – 11G) maintaining an accidental COR or disposing of it; * Item 18(a) – creating a COR and ensuring that it cannot be tampered with; * Items 18(b) – 18(e) – required components of the COR; * Item 19 – making CORs available to agency program and enforcement staff; * Item 20 – maintaining the COR to ensure its security and integrity.   **Uncompromised e-signature devices:** The system can assure that an e-signature was created by an individual named as the signer only if it can assure that the e-signature device used to execute the signature was uncompromised, remaining within the exclusive control of that individual. Assuring that the e-signature device is uncompromised requires protecting the device itself; it also requires identity-proofing the individual who is assigned the device, since determining that a device is within the exclusive control of an individual named as signer requires identifying the individual to whom the device was assigned. In addition, protecting the device requires protecting the associated user account, since access to that account can provide access to the device itself. The Checklist addresses these requirements in:   * Item 1 – identity-proofing of the individual who will be assigned an e-signature device; * Item 3 –   + (3A – 3D) assigning an e-signature device exclusively to an individual and assuring that the device is sufficient strong;   + (3E – 3G) ensuring that the individual assigned an e-signature device has been identity-proofed;   + (3H – 3K) ensuring that that the process of assigning a device protects it from compromise;   + (3L – 3N) protecting the e-signature device from unauthorized changes;   + (3O – 3P) protecting the account associated with the device from any tampering with the user’s contact information; * Item 4 – (4A) in the ESA, the signer agreeing to “promptly report to the agency or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised”; * Item 12 – automatically acknowledging e-signed submissions; * Item 13c – preventing e-signature device compromise with two-factor authentication and with measures to prevent guessing of device components; * Item 15 – flagging spurious e-signature device use; * Item 16 – revoking or rejecting compromised e-signature devices; * Item 17 – (17A – 17C) validating digital signatures, by determining that the signature was created using the private key associated with the named signer’s public key; * Item 18bB – including e-signatures in CORs in a way that protects them from compromising the e-signature devices used to execute them.   **Submitter/signer access what was submitted/signed:** A signature does not indicate certification to the truth or accuracy of a submission unless, prior to signing, the signer has access both to the submission content and to the certification statement – since the signer cannot intend the certification without some way of knowing what he or she is certifying to. In addition, whether an e-document is signed or not, the corresponding COR cannot be assured of representing the intended submission unless the submitter/signer can access the COR and repudiate it if appropriate, and unless there is a way to distinguish accidental submissions from intentional ones. The Checklist addresses these requirements in:   * Item 6 – providing opportunity for signers to review document content; * Item 7 – providing opportunity for signers to review certification statements and warnings; * Item 9 – providing opportunity for signers and submitters to view the COR; * Item 10 – addressing submitter/signer COR repudiation; * Item 11 – flagging accidental submissions; * Item 18e – providing CORs in a human-readable format, so that submitters’ and signers’ access to a COR allows them to know its content.   **Solution Building Blocks**  To meet these general and other requirements, the Checklist solutions often involve, and in some cases require, the use of **three general building blocks**: encryption, system logging, and system notifications and acknowledgements.  **Encryption:** For CROMERR purposes, encryption provides tools to protect secrecy, thus helping to protect signature device components from compromise. Encryption also offers tools for mathematically “fingerprinting” a file or other digital object, therefore providing a way to show that COR integrity requirements have been met.  Encryption always relies on some form of mathematical *algorithm*, as a method of calculating an artifact from the digital value of the content being encrypted. In addition, encryption may use *key(s)*, particularly where there is a need to decrypt the artifact, to recover the original content. Where encryption is used to “fingerprint” a file, the calculated artifact is typically a *hash value* (or *hash*). The hash provides this “fingerprint” because of its unique relation to the file: were the file to change, another application of the hashing algorithm would produce a different hash value than the original. So, for example, calculating a hash value today that is identical to one calculated yesterday provides mathematical certainty that the hashed file has not changed between yesterday and today. Hashing and key-based encryption are combined in the execution of *digital signatures*. Digital signatures use *private-public key cryptography*, which relies on two keys mathematically related so that what the one encrypts only the other can decrypt and vice versa. A digital signature is created by calculating a hash value for the e-document content being signed, and then using one of the keys (the private key) to encrypt the hash value. Digital signatures and procedures for their validation are discussed further under Item 17.  The following Checklist items and questions address encryption-based solutions:   * Item 3 –   + (3C – 3D) keys as signature device components;   + (3F) keys to secure access to a website;   + (3H) transmission security;   + (3K) protecting the secrecy of signature device components; * Item 5 – (5H – 5K) hashing to fingerprint the content of the COR; * Item 8 – (8A – 8C) transmission security and error checking; * Item 13b – (13bA) protecting the secrecy of signature device components; * Item 17 – digital signatures; * Item 18a – (18aA – 18aD) hashing to fingerprint the content of the COR; * Item 18bB – protecting the secrecy of signature device components.   **System logging:** System logs provide evidence of what transactions have occurred and how they occurred, which may help demonstrate that CROMERR requirements have been met. For example, rigorous logging of any processing of, or changes to, a COR may help provide COR integrity and may be used to show that this requirement is satisfied. Similarly, logging of users’ access to their accounts may help show how the system meets requirements for COR accessibility. The following Checklist items and questions address some of the possible uses of logging:   * Item 1 – (1G, 1biC) documenting the verification of registrants’ identities; * Item 5 – (5J) providing a repository for COR hash values; * Item 8 – (8F, 8G) documenting transmission errors and the system’s responses; * Item 12 – (12D) documenting the automated acknowledgement of an e-signed submission; * Item 15 – (15E) documenting a pattern of transactions that might indicate fraud; * Item 18 – (18aC) providing a repository for COR hash values; * Item 20 –   + (20B, 20J) documenting changes to CORs being maintained by the system;   + (20F) documenting system security breaches.   **System notifications and acknowledgements:** Notifications and acknowledgements sent to signers and submitters of e-documents empower them to help ensure the system meets CROMERR requirements. For example, the required automated acknowledgement of e-signed submissions gives signers a way to discover that spurious signatures have been executed in their names, showing that their e-signature devices have been compromised. Similarly, the required notifications that CORs are available for review is part of the process that signers and submitters use to determine whether the CORs represent their intended submissions and certifications. The following Checklist items and questions address some of the possible or required notifications and acknowledgements, informing signers or submitters that:   * Item 2 – (2F) their signing authority has been revoked; * Item 3 –   + (3L) their e-signature devices have been changed;   + (3O) their user account contact information has been changed; * Item 8 –   + (8E) there were errors in the transmission of submissions;   + (8G) their submissions have been rejected because of transmission errors; * Item 9a – **[required]** CORs of their submissions are available for their review; * Item 10 –   + (10F) the system is (or is not) allowing the repudiation of a COR;   + (10 J – L) a repudiated COR has been corrected or deleted; * Item 11 – (11E) the system has flagged one of their submissions as accidental; * Item 12 – **[required]** one of their e-signed submissions has been received; * Item 15 –   + (15B) their reports of e-signature device compromise have been received;   + (15F) the system has flagged one of their e-signatures as spurious; * Item 16 – (16F) their e-signature devices have been suspended or revoked; * Item 17 – (17B, 17E) one of their digital signatures has been successfully (or unsuccessfully) validated. | | | |
| **CROMERR Terms**  compromised – an electronic signature device is *compromised* if the code or mechanism is available for use by any other person than the individual uniquely entitled to use it.  copy of record (COR) *–* 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.  electronic document (e-document) *–* any information in digital form that is conveyed to an agency or third-party, where ‘‘information’’ may include data, text, sounds, codes, computer programs, software, or databases. ‘‘Data,’’ in this context, refers to a delimited set of data elements, each of which consists of a content or value together with an understanding of what the content or value means; where the electronic document includes data, this understanding of what the data element content or value means must be explicitly included in the electronic document itself or else be readily available to the electronic document recipient.  electronic document receiving system *–* any set of apparatus, procedures, software, records, or documentation used to receive electronic documents.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information.  electronic signature agreement (ESA) -- 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.  electronic signature device (e-signature device) *–* 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.  valid electronic signature (valid e-signature) –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. | | | |
| **Cases:**   * System receives submissions with e-signatures.   + Checklist must address all of the section 3.2000(b) requirements.   + GO TO **Registration**. * System receives submissions signed only with follow-on handwritten signatures on paper.   + Checklist must address the (B) *Signature*, (C) *Submission*,and (E) *COR* requirements.   + GO TO **Signature Process**. * System receives only submissions without signatures.   + Checklists must address (C) *Submission* and (E) *COR* requirements.   + GO TO **Submission Process**. | | | |
| **Registration (e-signature cases only)**  [**Return to Top**](#TOC) | | | |
| Checklists for systems that will receive submissions with e-signatures need to describe their registration process. CROMERR *Registration* requirements include:   * *Identity-proofing of registrant* (Item 1) – determining that registrants are who they claim to be.   Identity-proofing is the only case where CROMERR requirements vary depending on whether submissions are priority reports. Where registrants will sign priority reports, then identity-proofing must occur before the system begins accepting reports signed by the registrant. In addition, the identity-proofing process must either be by attestation of disinterested individuals based on information or objects of independent origin, or else by submission of subscriber agreements with handwritten signatures. The subscriber agreements are submitted either to the agency or to a local registration authority (LRA) that forwards a corresponding agreement collection certification to the agency.  CROMERR *Registration* requirements also include:   * *Determination of registrant’s signing authority* (Item 2) – determining that registrants have signatory authority for the submissions they are registering to sign.   + Item 2 includes determining a registrant’s relationship to the entities for which he or she will be signing submissions. * *Establishment of an e-signature device for the registrant in a way that protects it from compromise* (Item 3) – ensuring that only the identified registrant has access to the e-signature device and user account that is assigned to him or her. * *Electronic signature agreement* (Item 4) – having the registrant sign an agreement to terms and conditions for using an e-signature device.   + Item 4 may be satisfied as a part of satisfying Item 1.   **The Checklist must describe how these registration requirements are satisfied for any individual who will electronically sign e-documents submitted to the system.** | | | |
| **CROMERR Terms**  agreement collection certification – 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.  compromised – an electronic signature device is *compromised* if the code or mechanism is available for use by any other person than the individual uniquely entitled to use it.  disinterested individuals – 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.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information.  electronic signature device (e-signature device) *–* 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.  electronic signature agreement (ESA) -- 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.  handwritten signature -- the scripted name or legal mark of an individual, handwritten by that individual with a marking-or writing- instrument such as a pen or stylus and executed or adopted with the present intention to authenticate a writing in a permanent form, where ‘‘a writing’’ means any intentional recording of words in a visual form, whether in the form of handwriting, printing, typewriting, or any other tangible form. The physical instance of the scripted name or mark so created constitutes the handwritten signature. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other media.  information or objects of independent origin – data or items that originate from a disinterested individual or are forensic evidence of a unique, immutable trait which is (and may at any time be) attributed to the individual in whose name the device is issued.  local registration authority (LRA) – 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.  priority reports – the reports listed in Appendix 1 to part 3.  subscriber agreement – 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. | | | |
| **Item 1: Identity-proofing of registrant**  [**Return to Top**](#TOC) | | | |
| **General Requirements:**  The identity of registrants who will electronically sign e-documents submitted to the system must be determined with “legal certainty”. This requirement is more stringent and specific where the system will accept electronically signed priority reports.   * For registrants who will sign priority reports, CROMERR requires that the system establish their identity before accepting documents with their e-signatures. There are two ways to do this:   + Verification and attestation of identity by a disinterested party, based on information or objects of independent origin – at least one of which is government-issued.   + Submission of an electronic signature agreement (ESA) in the form of a subscriber agreement signed with the registrant’s handwritten signature. * For registrants 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. | | | |
| **Cases:**   * System will not accept priority reports.   + Item 1 must describe how system determines identity of registrant.   + GO TO **Non-Priority: Identifying Information**. * System will accept priority reports.   + Item 1 must describe how system determines the identity of registrant, both:     - before accepting documents with their e-signatures;     - with methods specified under section 3.2000(b)(5)(vii)(A), (B) or (C).   + GO TO **Item 1a**. | | | |
| **Non-Priority: Identifying Information** | |  | |
| **1A** | What forms of identification do registrants submit? *Examples:* driver’s license numbers, credit card numbers, passport numbers, and tax identification numbers. | | |
| **1B** | Are the identifications unique to an individual? *Examples:* government-issued identifications are; physical and email addresses may not be. | | |
| **1C** | Are the identifications durable (not subject to change)? *Examples:* government-issued identifications are generally durable; IP addresses are not; physical addresses and credit card numbers may not be. | | |
| **Non-Priority: Verification** | |  | |
| **1D** | Are registrants’ identities verified based on what they submit?   * How is verification done? *Examples:* DMV confirmation of driver’s license number match with other submitted registrant information; in-person inspection of government-issued picture identifications; telephone confirmation of registrant information with employer. | | |
| **1E** | Who performs the verification? Does this person meet the definition of a disinterested individual? “Disinterested individual” means 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, 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. *Examples:* State environmental agency staff, another State agency, a third-party vendor, automated processes. | | |
|  |  | | **NEXT** **Item 2** |
| **Item 1a: (priority reports only) Identity-proofing *before* accepting e-signatures** | | | |
| **Requirements:**  Identity-proofing must be completed before the system accepts any priority report documents signed by the registrant. | | | |
| **1aA** | **Review** Are all elements of the identity-proofing process completed for a registrant before the system accepts documents electronically signed by that individual? | | |
| **Item 1b: (priority reports only) Identity-proofing method** | | | |
| **Cases:**   * System will use identity-proofing methods that do not rely on paper documents.   + These are the methods specified under section 3.2000(b)(5)(vii)(A) and (B).   + GO TO **Item 1bi**. * System will use identity-proofing that relies on paper documents.   + This is the subscriber agreement method provided by section 3.2000(b)(5)(vii)(C).   + GO TO **Item 1b-alt**. | | | |
| **Item 1bi: (priority reports only) Verification by attestation of disinterested individuals** | | | |
| **Requirements:**  The registrants’ identities must be verified by disinterested individuals who attest to the verification. | | | |
| **1biA** | Are registrants’ identities verified based on what they submit?   * How is verification done? *Examples:* DMV confirmation of driver’s license number match with other submitted registrant information; in-person inspection of government-issued picture identifications; telephone confirmation of registrant information with employer. | | |
| **1biB** | Who performs the verification? *Examples:* State environmental agency staff, another State agency, a third-party vendor, automated processes.   * **Are these disinterested individuals?** | | |
| **Item 1bii: (priority reports only) Information or objects of independent origin** | | | |
| **Requirements:**  Verification of the registrants’ identities must be based on their submission of “information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization.” | | | |
| **1biiA** | What forms of identification do registrants submit? *Examples:* driver’s license numbers, credit card numbers, passport numbers, tax identification numbers.   * Do any of the items submitted meet the CROMERR requirement that they be “information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization”?   + If no item meets this requirement, are there items that provide equally strong evidence of the registrant’s identity? | | |
| **1biiB** | Are the identifications unique to an individual? *Examples:* government-issued identifications are; physical and email addresses may not be. | | |
| **1biiC** | Are the identifications durable (not subject to change)? *Examples:* government-issued identifications are generally durable; IP addresses are not; physical addresses and credit card numbers may not be. | | |
|  | | **NEXT Item 2** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1b-alt: (priority reports only) Subscriber agreement alternative** | | | | |
| **Requirements:**   * Subscriber agreements must contain the three required elements of ESAs (see Item 4). * The original paper copy of the agreement, with its handwritten signature, must be stored for at least five years after the associated signing credential has been deactivated. | | | | |
| **Cases:**   * Registrants will submit subscriber agreements to the system.   + System must receive and maintain original copies of subscriber agreements.   + GO TO **Submission Option: Content**. * Subscriber agreements will be received and maintained by a local registration authority (LRA).   + System must receive and maintain certifications from LRA that subscriber agreements have been received and are being maintained.   + GO TO **LRA Option**. | | | | |
| **Submission Option: Content** | | |  | |
| **Submission Option: Delivery and Review** | | |  | |
| **Submission Option: Maintenance** | | |  | |
| **1b-altA** | | Are the original paper copies of the subscriber agreements retained and stored?   * **Are these copies stored for at least five years after the associated signing credential has been deactivated?** * Are these copies stored in a way that protects them from tampering, destruction and unauthorized access? | | |
|  | | **NEXT Item 2** |
| **LRA Option:****LRA Establishment** | | |  | |
| **1b-altB** | | What individuals are or will be authorized as LRAs? | | |
| **1b-altC** | | What form of affidavit is required from individuals who will serve as LRAs?   * How does the affidavit establish the identity of these individuals? * How is the affidavit furnished to the state system?   Note to reviewer: It is assume that the attestation will be electronic. | | |
| **LRA Option: Certification Content** | | |  | |
| **1b-altD** | | Do LRAs submit an agreement collection certification (“certification”) for each subscriber agreement they receive?   * What does the certification contain? | | |
| **LRA Option: Certification Review/Recording** | | |  | |
| **1b-altE** | | How does the state/system collect and preserve the certification statements from the LRA? | | |
| **LRA Option: Agreement Content** | | |  | |
| **LRA Option: Agreement Maintenance** | | |  | |
| **1b-altF** | | How does the system ensure that the LRA maintains subscriber agreements:   * For at least five years after the associated signing credential has been deactivated, and * In a way that protects them from tampering, destruction and unauthorized access? * Are the original, paper agreements stored or otherwise archived? For example, are the originals scanned and then destroyed? | | |
| **Item 2: Determination of registrant's signing authority**  [**Return to Top**](#TOC) | | | | |
| **Requirements:**  Registrants who will electronically sign e-documents submitted to the system must be determined to have the authority to sign those documents. This involves determining the registrant’s relation to the company (or other entity) on whose behalf he or she will be signing. | | | | |
| **Determining Authority** | | |  | |
| **2A** | What kind of information is used to determine the registrant’s authority to sign e-documents submitted to the system? *Examples:* Statements or certifications from the registrant; statements or certifications from officials of the company for which the registrant will sign the e-documents; information in agency databases; other, publicly available information. | | | |
| **Verifying Authority** | | |  | |
| **Revoking Authority** | | |  | |
| **2B** | Does the system include a process to revoke the registrant’s authority?  Note to Reviewers: Reviewers will assume that the system inactivates user signature credentials and access when authorization is revoked unless the CROMERR application indicates otherwise. | | | |

|  |  |  |
| --- | --- | --- |
| **Item 3: Issuance (or registration) of a signing credential in a way that protects it from compromise**  [**Return to Top**](#TOC) | | |
| **Requirements:**  The registration process must establish an electronic signature device that uniquely belongs to the registrant, who will use it to electronically sign e-documents submitted to the system. **To meet CROMERR second-factor authentication requirements, the device must include two independent, differing types of components.** One of these will usually be a code, such as a PIN or password, and this may be created by the system. The other component will typically be something the registrant already possesses: items of personal knowledge; biometrics, such as fingerprints or scanned retinal images; or a hardware token, such as a USB drive or smart card.  Whatever the components, the general requirement is that they be established in a way that protects them from compromise. With the exception of hardware tokens and certain biometrics, these components depend on their secrecy to keep them from compromise, since anyone who knows a code or piece of personal information may use it to execute a signature. So, protection from compromise generally involves protecting component secrecy, and this requires the system to address following four more specific issues:   * *Component Strength* – component weakness must not expose them to unauthorized access, for example, through guessing or discovery with the aid commonly available “hacking” tools;      * *Registration Integrity* – device components must be established only for the registrant who undergoes the identity-proofing process described under checklist Item 1, and the registration process must not expose these components to unauthorized access; * *Maintenance Integrity* – system records of device components must not expose them to unauthorized access * *Account Integrity* – the registrant’s user account must be protected against unauthorized changes that could make device components associated with the account available to someone other than the registrant. | | |
| **Component Strength** | |  |
| **3A** | What are the signature device components?   * For each component, is it unique to the registrant?   + How does the system determine or ensure uniqueness? | |
| **3B** | Does the system use any additional devices to secure access to the registrant’s user account, such as a username and login credentials?   * If none of the device components under 3A are unique, does the system ensure that any of these additional devices are unique to the registrant? If so, how? | |
| **3C** | For each component, what standard of strength does it meet?   * **For PINs and passwords** –   + Is there a requirement for minimum length?   + Are there compositional requirements:     - For mixing numbers and letters and upper and lower case?     - For using special characters?     - For avoiding recognizable words? * **For challenge questions/answers** –   + How many challenge questions/answers does a registrant provide? [NOTE: EPA recommends at least five.]   + Does the system provide a list of questions from which the registrant chooses those he or she will answer?     - How many questions are on the list? [EPA recommends at least ten.]     - Does the list avoid questions whose answers can be easily guessed or learned by others?     - Do the available questions call for items of information normally committed to long-term memory?   + Does the system allow (or require) the registrant to provide his or her own questions to answer? * **For cryptographic keys (for example, associated with digital signatures)** –   + What key size is required?   + What applicable cryptographic standards are required to be met?   + Is access to the key – the private key, in the case of a digital signature – protected with a PIN/password or a hardware token?     - If it is a PIN/password, does this meet the component strength requirements for PINs and passwords (above)?     - If it is a hardware token, does this meet the hardware token strength requirements (below)?   + How is the key protected from being copied or transferred from the hardware unit on which it resides (the signer’s computer, smartcard, USB, etc.) to another?   + For cases where the certificate is on the agency server, how does the system ensure that the related certificate cannot be used by anyone other than the registrant?      * **For biometric components** –   + What is the method of biometric capture?   + How does biometric capture ensure that the biometric cannot be “spoofed”?   + What, if any, applicable standards are required to be met?   + What peer-reviewed studies have validated this technology?   + What rate of false positives and false negatives are generated by the biometric device that would be used. * **For hardware tokens** –   + What kind of access control is required for the token?     - If control is provide by a PIN/password, does this meet the component strength requirements for PINs and passwords (above)?   + Is the token subject to any technical standards? | |
| **3D** | For each component, how does the system enforce standards for strength? Note to reviewers: Reviewers will assume the systems reject substandard credentials and deny users access to the system if they submit substandard credentials, unless the CROMERR application indicates otherwise.  **For challenge questions/answers** –   * + Does the system reject answers that are too weak, for example, containing less than three characters?   + Does the system reject repetitions of the same answer for different questions?   + Where the registrant provides his or her own questions:     - Does the system reject repetitions of the same question?     - Does the system reject questions whose answers are easily guessed or learned?       * How does the system make this determination?   + What is the consequence of challenge question/answer rejection? * **For biometric components** –   + Does the system always accept the biometric that the registrant provides?   + If not, what the bases and consequences of rejection? * **For hardware tokens** –   + How does the system determine that the registrant has a token of the required type? | |
| **Registration Integrity: Process Linkage** | |  |
| **3E** | How does the system ensure that only the registrant who has been identity-proofed has access to the signature device registered in his or her name?   * What are steps in the process that provide this assurance? * What are the links between the device establishment process and the identity-proofing process?   + Do the links rely on the registrant’s control of access to his or her email account?   + Do the links rely on the integrity of the USPS?   + Do the links rely on some sort of code or cryptographic key?     - If so, how is the code or key provided, and how is it protected from compromise? | |
| **3F** | How does the system ensure that account contact information belongs to the registrant who has been identity-proofed? For example, if the system sends the user a link to first login and change password (after registration), that would suffice. If the system doesn’t do that, an email with a code would be sent to the user and the code should be entered upon first login. | |
| **Registration Integrity: Security** | |  |
| **3G** | Where signature device components are created or exchanged on-line, how are the sessions secured? *Examples:* SSL, TLS.   * What is the technology/version used? * If they do not use SSL or TLS, then how are the sessions secured? | |
| **3H** | Are electronic signature device components ever provided (or registered) off-line? *Examples:* By email, by USPS. If so –   * How are these transactions secured against interception? | |
| **Registration Integrity: Hardware Tokens** | |  |
| **3I** | For hardware token components, how does the system identify the particular token in the possession of the registrant, so that its use to execute signatures can be recognized? | |
| **Maintenance Integrity** | |  |
| **3J** | For each signature device component:   * Who has access to it? *Examples:* Database and system administrators, support staff. * Can components be deleted and replaced? If so, is there a read-only mechanism in place to demonstrate whether or not deletion/substitution has occurred? For example, is a read-only log kept of access to signature device components? * Is it maintained in an encrypted format? If it is –   + When is it encrypted?   + How is it encrypted, and with what algorithm?   + How is the encryption key protected from disclosure?   + Is it ever decrypted? * If it is not encrypted, how does the system prevent its disclosure and unauthorized use? | |
| **Account Integrity: Signature Device Changes** | |  |
| **3K** | Are account owners allowed to change their signature device components? *Examples:* Change a password, providing an answer to a different challenge question. If they are:   * Are they required to authenticate themselves to the system by entering their original signature device and/or other credentials?   + What is the authentication process? * Are the new components subject to the same strength requirements imposed on the originals?   + How are the strength requirements enforced? * Are the device changes provided with the same security that was required when the original components were created or registered? (See Questions 3H and 3I, above.) * Do account owners receive email notification of any device changes? | |
| **3L** | What happens in cases where an account owner forgets or otherwise loses his or her signature device components?   * Does the account owner have to re-register, and, in effect, establish a new account? * If the account owner does not have to re-register, how does the system ensure that the establishment of a new device meets the *component strength* and *registration integrity* requirements discussed above? | |
| **Account Integrity: Contact Information Changes** | |  |
| **3M** | Are account owners allowed to change account contact information, including their email addresses? If they are:   * What is the change process?   + How does the change process ensure that only legitimate account owners are able to make such changes?   + Are they required to authenticate themselves to the system by entering their signature device and/or other credentials?   + Is phone confirmation of requested changes required?   + Are notifications of changes sent to both the old and the new contact addresses? For example, if an email address is changed, is an email sent to both the new and old email addresses?   Note to reviewers: Reviewers are to assume that, if accounts owners are not allowed to change contact information, they must re-register with new contact information using the full registration process described under Items 1-4. | |
| **Item 4: Electronic signature agreement**  [**Return to Top**](#TOC) | | |
| **Requirements:**  Registrants must sign an ESA with respect to the electronic signature device established as discussed under Item 3, stating that the registrant will: (1) protect the device from compromise, (2) promptly report any evidence of compromise to the agency or agencies relying on the system, and (3) “be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature.” ESA’s may be executed on paper with handwritten signatures; they are then subscriber agreements, and are addressed under Item 1b-alt of the checklist. Otherwise, they are executed electronically, on-line. | | |
| **4A** | Does the ESA contain the registrant statement with the three required elements? (1. Protect the electronic signature device from compromise; 2) to promptly report to the agency or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised; and 3) to be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature). | |
| **4B** | How is the ESA electronically signed?   * Does the registrant use the electronic signature device established for his or her account? * If this device is not used, how does the system ensure that the ESA has been signed by the registrant and not by someone else? | |

|  |  |  |
| --- | --- | --- |
| **Signature Process**  [**Return to Top**](#TOC) | | |
| Signatures represent the signer’s agreement and certification to the content of the documents being signed. So, systems that will receive signed e-documents need to ensure that the content of the document as it is received and maintained is identical to the document content agreed to and certified to by the signer. The checklist addresses this in the following item:   * *Binding of signatures to document content* (Item 5) – providing a way to demonstrate that the e-document received and maintained is identical to the content agreed to and certified to by the signer.   Where the signature is an e-signature, signature binding must address the creation of a copy of record (COR) that represents the official system copy of the content agreed to and certified by the signer.  Whether the signature is an e-signature or is executed as a handwritten signature on a follow-on paper document, it can represent agreement and certification to document content only if the signer knows what that content is and understands what his or her signature means. So, checklists must also describe how the system provides the signer with both:   * *Opportunity to review document content* (Item 6), and * *Opportunity to review certification statements and warnings* (Item 7). | | |
| **CROMERR Terms**  copy of record (COR) *–* 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.  electronic document (e-document) *–* any information in digital form that is conveyed to an agency or third-party, where ‘‘information’’ may include data, text, sounds, codes, computer programs, software, or databases. ‘‘Data,’’ in this context, refers to a delimited set of data elements, each of which consists of a content or value together with an understanding of what the content or value means; where the electronic document includes data, this understanding of what the data element content or value means must be explicitly included in the electronic document itself or else be readily available to the electronic document recipient.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information.  handwritten signature -- the scripted name or legal mark of an individual, handwritten by that individual with a marking-or writing- instrument such as a pen or stylus and executed or adopted with the present intention to authenticate a writing in a permanent form, where ‘‘a writing’’ means any intentional recording of words in a visual form, whether in the form of handwriting, printing, typewriting, or any other tangible form. The physical instance of the scripted name or mark so created constitutes the handwritten signature. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other media. | | |
| **Item 5: Binding of signatures to document content**  [**Return to Top**](#TOC) | | |
| **Requirements:**  Generally, the requirement to bind signatures to document content is the requirement to ensure that what the signer agreed to and certified to is identical to the document content the system receives and maintains. Describing how this requirement is satisfied generally involves describing at least the following four things:   * *The signature* – what constitutes the signature as it is executed with respect to the submitted e-document; * *The signature process* – how and when the signature is executed. Where the signature is electronic, CROMERR requires that it be executed with two independent, differing types of signature device components; * *The system’s COR for the submission* – when and how the COR is created and what it includes. Where the signature is electronic, CROMERR requires that it be contained in the COR;   *The COR’s integrity –* how the system ensures that the document content included in the COR is identical to the content agreed to and certified to by the signer. | | |
| **Signature** | |  |
| **5A** | **For e-signatures**, what combination of components constitutes the signature? | |
| **5B** | **For follow-on paper signatures**, what is the format of the signature document?   * Beyond the handwritten signature itself, what elements does the document include that identify the signer and the document content being agreed to and certified to? | |
| **Signature Process** | |  |
| **5C** | **For e-signatures**, what does the signer do to execute his or her signature?   * What are the steps in the process? * When do these steps occur, relative to other parts of the submission process? * How does the system determine that the signing credential was not compromised upon first use?   For example, for password protected processes, is a second independent authenticating factor for the signature device components used?   * What happens if the signer is unable to supply the correct device component when prompted – for example, forgetting his or her PIN, or answer to a challenge-question?   + How many attempts is the signer allowed?   + What happens after the signer makes the allowed attempts and fails? * At what point in the process is execution complete? * How does the signer know that signature execution is complete? | |
| **5D** | **For** **e-signatures** where the process involves several steps:   * Does the system time-out if the signer client is inactive for a period of time?   + What is the time-out threshold? * If the system does not time-out, how does the system prevent the signer from entering signature device components and then walking away, so that an unauthorized individual can complete the signature process? | |
| **5E** | **For follow-on paper signatures**:   * Is there anything in the signature document that links it to the time of e-document submission? * How is the signature document sent? * Is there a deadline for receipt of the signature document? * What happens if the signature document is not received? | |
| **COR** | |  |
| **5F** | What are the components of the COR?   * In what format is the submitted document content included? * What meta-data elements are included? *Examples:* Date/time of receipt; network data, such as source IP address; system error-checking data; cryptographic elements, such as a content hash; information necessary to record the meaning of the document content, such as style sheets for XML-formatted content. * Does it contain document attachments?   + In what format are these included?   + How are these linked to the document content? * **For** **e-signatures**, what signature components does it contain? * **For follow-on paper signatures**, does the COR contain any components that cross-reference the signature document? If so, what are these components? | |
| **COR Integrity** | |  |
| **5G** | Does the system calculate a cryptographic hash value of some or all of the COR, to ensure that the hashed components remain unchanged since signature execution? If so –   * When is the hash value calculated? *Examples:* Before the document is submitted; before the e-signature is executed; after the document is received; after the e-signature is executed. * Are all the components of the COR hashed? If some components are not hashed:   + Which ones are not hashed?   + How does the system show that these remain unchanged since signature execution? * Are the COR components hashed together to produce one hash value, or are they hashed separately to produce a hash value for each component? If they are hashed separately, what ensures that one cannot be changed independently of the other? * What is hashing or digital signature algorithm used to produce the hash? *Examples:* SHA-2, RSA, DSA, ECDSA.   + Is the algorithm currently FIPS approved? [Note that SHA-1 is not FIPS approved.] * If hash calculation requires a key, how is the key protected from unauthorized access? * Is the hash calculated in conjunction with executing a digital signature? If so –   + How are the private/public keys generated?   + Are the keys associated with a Public Key Infrastructure (PKI) certificate?   + How are private keys protected from unauthorized access? | |
| **5H** | Does the system use some other (non-hash-related) cryptographic process to secure COR components?   * What is the process? * How does it secure COR components? * How is access to the process, and any keys it may involve, protected from unauthorized access? | |
| **5I** | How are hash values (or other cryptographic artifacts) secured from tampering – so that COR components cannot be changed and hash values replaced without detection?   * Is the protection of the hashing key (or PKI private key) sufficient to ensure that hash values cannot be recalculated to conceal changes to the hashed components? * Where is the hash value stored?   + If it is stored in a database, how is access to the hash value controlled?   + Is the hash value included in the COR?   + Is the hash value included in a submission log that is secured from tampering?     - How is the log secured? | |
| **5J** | If COR components are not hashed or secured with some other cryptographic process, how can the system show that COR components remain unchanged since signature execution?   * Is the submission file “locked” in some way, so that any change would be detectable? * Is the COR maintained in a database that protects it from tampering, or from deletion and replacement?   + How does the database provide this security? | |
| **Item 6: Opportunity to review document content**  [**Return to Top**](#TOC) | | |
| **Requirements:**  The system must provide the signer with the opportunity to review the content of the document being submitted in a human readable format. | | |
| **6A** | Does the system provide the signer with the opportunity to review the content of the document being submitted?   * When is this opportunity provided?   + **For** **e-signatures**, is this provided before signature execution?   + **For follow-on paper signatures**, is this provided before or after document submission? * How is this opportunity provided?   + Is it provided on-line?   + Is it provided off-line, via a downloaded file?   + Is it provided in some other way? * What format does the system provide for the document content being reviewed?   + Does the COR include evidence of the format provided? | |
| **Item 7: Opportunity to review certification statements and warnings**  [**Return to Top**](#TOC) | | |
| **Requirements:**  Before executing their signatures, the system must give signers the opportunity to review any applicable certification statements, including any applicable warnings that false certification carries criminal penalties. | | |
| **7A** | Does the system give signers the opportunity to review any applicable certification statement – including any applicable warnings that false certification carries criminal penalties – before they execute their signatures? | |

|  |  |  |
| --- | --- | --- |
| **Submission Process**  [**Return to Top**](#TOC) | | |
| A CROMERR-compliant e-document receiving system must assure *message integrity*, that is, that the document content received is identical to the content that was sent by the submitter. The checklist addresses this in:   * *Transmission error checking and documentation* (Item 8).   In addition, the system must be able to show that the submission was *intentional* – that both the content and its submission were what the submitter and any signer intended – and must allow the submitter/signer to repudiate the submission in case it was unintended. The checklist addresses these requirements in:   * *Opportunity to review copy of record* (Item 9); * *Procedures to address submitter/signatory repudiation of a copy of record* (Item 10); and * *Procedures to flag accidental submissions* (Item 11).   Finally, in cases of e-signature, the system must provide a way for signers to know that submissions were received with their signatures/certifications, even they do not access the copy of record for review. The checklist addresses this in:   * *Automatic acknowledgment of submission* (Item 12). | | |
| **CROMERR Terms**  copy of record (COR) *–* 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.  electronic document (e-document) *–* any information in digital form that is conveyed to an agency or third-party, where ‘‘information’’ may include data, text, sounds, codes, computer programs, software, or databases. ‘‘Data,’’ in this context, refers to a delimited set of data elements, each of which consists of a content or value together with an understanding of what the content or value means; where the electronic document includes data, this understanding of what the data element content or value means must be explicitly included in the electronic document itself or else be readily available to the electronic document recipient.  electronic document receiving system *–* any set of apparatus, procedures, software, records, or documentation used to receive electronic documents.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information. | | |
| **Item 8. Transmission error checking and documentation**  [**Return to Top**](#TOC) | | |
| **Requirements:**  The system must be able to:   * Prevent transmission errors; * Detect and document transmission errors, to the extent that they cannot be prevented; and * Reject submissions in which errors are detected, at least pending correction. | | |
| **Error Prevention** | |  |
| **8A** | Does the system use cryptographic technologies to protect the submission from errors and malicious tampering during transmission? *Examples:* SSL, TLS. If so –   * What technology/version is used? | |
| **8B** | If the system does not use cryptographic technologies, how are submissions protected from errors and malicious tampering during transmission? | |
| **Error Detection and Documentation** | |  |
| **8C** | How does the system detect transmission errors?   * Does the system rely on the same cryptographic technologies used to protect the submission during transmission? * If the system does not rely on the same cryptographic technologies used to protect the submission during transmission, does the system rely on the submitter/signer to check the received submission and report any errors? If so –   + How does the system ensure that error reports are actually from the submitter/signer?   + Does the system require that submitter/signer error reports be signed and certified?     - Does this involve the use of e-signatures? | |
| **8D** | Are system administrators notified of errors?   * How are they notified? | |
| **8E** | Are the submitters/signers notified of errors?   * How are they notified? *Examples:* By email, by telephone. | |
| **8F** | Are transmission errors documented in a system log? If so –   * What are the relevant data fields in the log? | |
| **Rejection of Documents with Errors** | |  |
| **8G** | For systems that do not use cryptographic technologies that automatically reject documents with errors (e.g., SSL and TLS automatically reject documents with errors) Does the system reject submissions with detected errors?   * + Reviewers will assume that notifications and documentation described above in Item 8 will also be applicable here. | |
| **8H** | If the system does not reject submissions with detected errors, how are errors corrected? | |
| **Item 9. Opportunity to review copy of record (See 9a through 9c)**  [**Return to Top**](#TOC) | | |
| **Requirements:**  The system must give the submitter/signer the opportunity to review a copy of record (COR) of his or her submission by:   * Notifying the submitter/signer that a COR is available (Item 9a), * Providing a human-readable format for the COR (Item 9b), and   Giving the submitter/signer access to the COR (Item 9c). | | |
| **Cases:**   * Checklist describes system that receives only submissions without signatures.   + GO TO **Item 9 General**. * Checklist describes system that receives signed submissions.   + GO TO **Item 9a**. | | |
| **Item 9a. Notification that copy of record is available** | | |
| **9A** | How is a submitter/signer notified that a COR is available for his or her review?   * Is the submitter/signer notified on-line? If so –   + Is notification provided outside the session in which the submission is made? * Is the submitter/signer notified off-line? If so –   + How is the notification provided? *Examples:* By email, by USPS.   + **For** **e-signatures**, is notification provided in the automatic acknowledgement of submission addressed under checklist Item 12? | |
| **9B** | If the submitter/signer is notified off-line:   * Is the notification sent to a pre-established address that cannot be changed during the on-line session in which the submission is made? * How is the pre-established address –   + Established in a way that ensures that it belongs to the submitter/signer? [**For** **e-signatures**, this may be addressed under Question 3G.]   + Protected from unauthorized modification? [**For** **e-signatures**, this may be addressed under Question 3O.] | |
| **Item 9b. Creation of copy of record in a human-readable format** | | |
| **9C** | How is the COR formatted for signer/submitter review?  If the COR is not included in the acknowledgement, is it available for viewing in a location from which it cannot be deleted? | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item 9c. Providing the copy of record** | | | | |
| **9D** | Is the submitter/signer given on-line access to the COR? | | | |
| **9E** | If the COR is provided off-line:   * Is the COR sent to a pre-established address that cannot be changed during the on-line session in which the submission is made? * How is the pre-established address –   + Established in a way that ensures that it belongs to the submitter/signer? [**For** **e-signatures**, this may be addressed under Question 3G.]   + Protected from unauthorized modification? [**For** **e-signatures**, this may be addressed under Question 3O.] | | | |
| **Item 10. Procedures to address submitter/signatory repudiation of a copy of record**  [**Return to Top**](#TOC) | | | | |
| **Requirements:**  The system must have procedures for repudiating a COR that provide for:   * *Repudiation notification* – submitter/signer notification that the COR does represent what he or she intended to submit; * *Repudiation determination* – system administrator decision to accept or reject the repudiation; * *COR correction* – the creation of a corrected COR; * *Original COR disposition* – the disposition of any records related to the COR as created for the original submission.   **To satisfy CROMERR requirements, the system must either retain original COR or maintain a record of the changes made to the original COR.** | | | | |
| **Repudiation notification** | | |  | |
| **10A** | If submitters/signers may repudiate their CORs on-line, are they allowed direct access to the existing CORs, to correct or delete them? If they are –   * How does the system protect the CORs from unauthorized changes by individuals who are neither signers nor submitters? | | | |
| **Repudiation determination** | | |  | |
| **10B** | How are notifications of COR repudiation determined to be authentic?   * If they are submitted on-line, does the submitter have to provide a PIN or password, or some other identifying information? * If they are submitted via email or on paper, what kind of identifying information or tokens does the submitter have to provide? * Do system administrator staff ever follow-up with a phone call to confirm the authenticity of the notification? If so –   + Who is called, and what is the source of the phone number used? | | | |
| **COR Correction** | | |  | |
| **10C** | When a COR is repudiated, is the existing COR corrected, or is a new COR created? | | | |
| **10D** | How are corrections to the COR submitted – electronically or on paper?   * If they are submitted electronically, does the submitter use the same submission processed used to submit the content of the original COR?   + If the submitter uses a different process –     - What is it?     - How does the process ensure that what the submitter submits is accurately represented by the corrected or new COR? * If they are submitted on paper –   + Is the revised COR created and maintained on paper?   + If the COR is still created and maintained electronically, how is the content submitted on paper converted to electronic media? | | | |
| **10E** | If the original COR included an e-signature, is a new e-signature executed with respect to the new COR content?   * If it is,   + Is the signature process the same as that for the original submission?   + Does the system satisfy the Item 5 requirements that the e-signature be bound to the new COR content? * If it is not, how does the system satisfy the Item 5 requirements that the e-signature be bound to the new COR content? | | | |
| **10F** | Is the submitter/signer notified of the COR correction or of the new COR?   * What does the notification contain? * To what address is the notification sent? * Does the notification inform the submitter/signer that the corrected or new COR is available for review? | | | |
| **Original COR Disposition** | | |  | |
| **10G** | | Is the original, repudiated COR retained by the system? If it is –   * Is it flagged as repudiated?   + If so, what constitutes the “flag”?   + If not, how does the system track the fact that this version is repudiated?   + Is the submitter/signer notified that the original COR is now tracked as repudiated in the system? * Where and how long is the repudiated COR maintained?   + Is it secured from tampering and other unauthorized access? | | |
| **10H** | | If the original COR is not retained by the system –   * Does the system maintain a record of the changes to the original COR, so that the content of the original can be reconstructed if necessary?   + Where and how long is the record maintained?   + Is it secured from tampering and other unauthorized access? * Is the submitter/signer notified that the original COR has been deleted from the system? | | |
| **Item 11. Procedures to flag accidental submissions**  [**Return to Top**](#TOC) | | | | |
| **Requirements:**  The system must either be able prevent accidental submissions – so that they do not need to be addressed – or else the system must address:   * *Accident mitigation* – measures that make accidental submissions an unlikely and infrequent occurrence; * *Accident detection* – quality and completeness checks that allow accidental submissions to be flagged; and * *COR Repudiation* – procedures to allow the submitter/signer to repudiate CORs resulting from accidental submissions that meet the requirements for any COR repudiation. | | | | |
| **Cases:**   * Checklist describes system functionality that prevents accidental submissions.   + GO TO **Prevention**. * System does not prevent accidental submissions.   + GO TO **Accident Procedures**. | | | | |
| **Prevention** | | |  | |
| **11A** | What measure does the system provide to prevent accidental submissions?  How do these measures prevent accidental submissions? | | | |
|  | | | **NEXT Item 12** |
| **Accident Procedures: Mitigation** | | |  | |
| **11B** | What factors in the system’s submission process make accidental submissions unlikely? *Example:* The process includes warnings and confirmatory steps before submission can be completed. | | | |
| **Accident Procedures: Detection** | | |  | |
| **11C** | What automatic quality and completeness checks does the system provide for submissions it receives? | | | |
| **11D** | Does the system use checks other than quality and completeness to flag accidental submissions? *Examples:* Submission timing, submission source. | | | |
| **11E** | Are submitters/signers notified when their submissions are flagged as accidental?   * If so, how are they notified? * Are submitters asked to make corrections, or simply to resubmit? | | | |
| **Accident Procedures: COR Repudiation** | | |  | |
| **11F** | Can submitters/signers repudiate a COR based on asserting that the submission was accidental?  Note to reviewers: Reviewers will assume the procedures are the same as described for repudiation under Item 10 unless the CROMERR application indicates otherwise. | | | |

|  |  |
| --- | --- |
| **12. (e-signature cases only) Automatic acknowledgment of submission**  [**Return to Top**](#TOC) | |
| **Requirements:**  Systems must respond to an e-signed submission with an acknowledgement that:   * Is sent automatically; * Identifies the e-document received, the signer, and the date and time of receipt; * Is sent to at least one address “that does not share the same access controls as the account used to make the electronic submission” (§3.2000(b)(5)(vi)).   This third requirement is sometimes referred to as sending the acknowledgement to an *out-of-band* address. | |
| **12A** | Does the system respond to every e-signed submission with an acknowledgement that is sent automatically?   * How is the acknowledgement sent? *Examples:* By email, by telephone, by fax, by USPS. |
| **12B** | Does the acknowledgement include:   * The name or other identifiers of the signers?   + If other identifiers are used, what are they? * An identifier of the e-document received that will be meaningful to the submitters/signers?   + What is this? * The date and time of the submission’s receipt?   Note to reviewers: Reviewers will assume that secret information such as password or private key is not included unless the CROMERR application indicates otherwise. |
| **12C** | Is the acknowledgement sent to an *out-of-band* address?   * What is the address? * What are the access controls for the address? |
| **12D** | Does the system document or log the acknowledgement? If so –   * Does the documentation/log include:   + The date/time the acknowledgement was sent?   + The address it was sent to?   + The contents? * How is the documentation/log protected from alteration or deletion? * How long is the documentation/log maintained? |
| **12E** | Does the system follow-up where the emailed acknowledgement notices are undeliverable?   * What are the follow-up procedures? |
| **12F** | If the COR is not included in the acknowledgement, is it available for viewing in a location from which it cannot be deleted? |

|  |  |  |
| --- | --- | --- |
| **Signature Validation (e-signature cases only)**  [**Return to Top**](#TOC) | | |
| Where the system receives submissions with e-signatures, it must be able to determine that those e-signatures were valid at the time of signing. As CROMERR defines it, a valid electronic signature must be created by a signer who was authorized to execute it (**authorization**) with an e-signature device that the signer uniquely owns (**ownership**) and that was uncompromised (**compromise**) at the time of signing. The checklist addresses **ownership** in:   * *Determination that credential is authentic* (Item 13a), which applies to cases where the e-signature device is provided (issued or registered) by a third party, and * *Determination of credential ownership*, which applies to cases where the e-signature device is provided by the system itself (Item 13b).   Systems protect against device **compromise** with measures to **prevent** it, to **detect** it where it occurs, and to **reject** compromised devices once they are detected. The checklist addresses these measures as follows:   * **Prevention –** *Determination that credential is not compromised* (Item 13c); * **Detection –** *Procedures to flag spurious credential use* (Item 15); and * **Rejection** – *Procedures to revoke/reject compromised credentials* (Item 16).   The checklist addresses **authorization** in:   * *Signatory authorization* (Item 14).   Finally, the checklist addresses an issue specific to digital signatures – that is, e-signatures using private/public-key cryptography – in:  *Confirmation of signature binding to document content* (Item 17). | | |
| **CROMERR Terms**  compromised – an electronic signature device is *compromised* if the code or mechanism is available for use by any other person than the individual uniquely entitled to use it.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information.  electronic signature device (e-signature device) *–* 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.  valid electronic signature (valid e-signature) –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. | | |
| **13. Credential validation (See 13a through 13c)**  [**Return to Top**](#TOC) | | |
| **Cases:**   * The system accepts only e-signatures executed with e-signature devices provided by the system itself.   + GO TO **Item 13b**. * The system accepts e-signatures executed with e-signature devices provided by a third party.   + GO TO **Item 13a**. | | |
| **13a. Determination that credential is authentic** | | |
| **Requirements:**  Where a system accepts e-signatures executed with e-signature devices provided by a third party, the system must be able to determine that a particular e-signature it receives was executed with a device that the third party recognizes as uniquely owned by the individual identified as the signer. | | |
| **13aA** | What is the third party that provides e-signature devices used to execute signatures accepted by the system?   * Is it a public key infrastructure (PKI) certificate authority? | |
| **13aB** | How does the system determine that the third party currently recognizes an e-signature device as belonging to an identified signer? | |
| **13aC** | What are the procedures where the third party does not recognize the e-signature device used to execute the signature? | |
|  | **NEXT Item 13c** |
| **13b. Determination of credential ownership** | | |
| **Requirements:**  Where a system accepts only e-signatures executed with e-signature devices provided by the system itself, the system must be able to:   * Determine that the device used to execute the signature matches the device the system uniquely associates with the identified signer, and   Make the determination without risk of compromising the device. | | |
| **13bA** | Where the e-signature is simply a token of the device, does the system compare the token to the corresponding device on file for the identified signer? For example, where the signature is created with a PIN, does the system simply compare the PIN included with the submission to the PIN on file for the signer?   * If the system does something else, what it is? * Does the system compare the encrypted versions of the values or the clear text versions?   + If the system compares clear text versions, how does the system control the risk of compromise posed by unauthorized access to the clear text?   + If the system uses encrypted versions, are the values encrypted by the signer’s computer prior to submission or by the system receiving the submission? * What are the procedures where the compared values do not match?   + Is the signer allowed to re-enter a token?     - How many tries is the signer allowed?     - What happens when the limit is exceeded with no match? | |
| **13bB** | Where the e-signature is a calculated artifact – such as a digital signature – what is the process for determining that the device used to execute the signature matches the device the system uniquely associates with the identified signer?   * For example, if the device includes a PKI certificate issued by the system, does the signer present his or her certificate to the system, or does the system rely solely on validating the signature with the public key on file for the signer, as described in checklist Item 17? * What are the procedures where the device does not match the device the system uniquely associates with the identified signer? | |

|  |  |  |  |
| --- | --- | --- | --- |
| **13c. Determination that credential is not compromised** | | | |
| **Requirements:**  To be able to determine that a credential is not compromised, the system must implement measures to **prevent** compromise, and these are addressed here. The system must also be able to **detect** compromise and have procedures to **reject** compromised credentials, and the checklist addresses these under Items 15 and 16.  To **prevent** compromise, the system must:   * Provide *two-factor authentication* for the e-signatures it accepts. Generally, two-factor authentication requires e-signature devices with two components of sufficiently different types. Where one of these is a secret code of some sort, such as PIN or password, the other might be an item of private personal knowledge – provided as the answer to a challenge-question – or a physical object, such as a smartcard, or a biometric;   Prevent *component guessing* – that is, attempts to guess secret codes or items of private personal knowledge. | | | |
| **Two-factor Authentication** | | |  |
| **13cA** | Does the system require that any PIN/password-based e-signature it accepts have attendant to it a device or mechanism that ensures that the password was not compromised at the time of use?   * What is the second authenticating factor? Does it effectively guard against a claim that a co-worker gained access to both authenticating factors in order to make an authorized statement to the government? * Do both components meet the strength requirements specified under Item 3? (See Question 3C.) | | |
| **Component Guessing** | |  | |
| **13cB** | For device components that are secret or private – such as PINs or answers to challenge-questions – does the system limit the number of failed attempt to provide the correct component?   * What is the limit? * Is the limit the same for each component, and, if not, why not?   + In the case of answers to challenge-questions, is each attempt prompted with a randomly selected question – or is it the same question each time? * Is the limit for a certain period of time? *Examples*: three attempts during a single session, three attempts within 24 hours. | | |
| **13cC** | What happens when the limit of failed attempts is reached?   * Is the user account associated with the identified signer locked?   + Does the account automatically unlock after the time period for the limit passes – for example, after the end of the user session, or after 24 hours?   + If the account does not automatically unlock, how does the user regain access to the account? * If the user account is not locked, what happens when the limit is reached? | | |
| **Item 14. Signatory authorization**  [**Return to Top**](#TOC) | | | |
| **Requirements:**  Based on records associated with the identified signer’s account, the system must determine that he or she is currently an authorized signer of the submission received with the signature. | | | |
| **14A** | Does the system use the records associated with the identified signer’s account – established and maintained as a part of registration (see Item 2) – to determine that he or she is currently an authorized signer of the submission received with the signature?   * If not, how does the system make this determination? | | |
| **14B** | What actions are taken if the identified signer is determined not to be a currently authorized signer? | | |
| **Item 15. Procedures to flag spurious credential use**  [**Return to Top**](#TOC) | | | |
| **Requirements:**  System must have some procedures to detect signature device compromise. The procedures may involve:   * *Collaboration with the device owners*, who are obligated under their electronic signature agreements to report any evidence of device compromise; * *Business process criteria*,to flag submissions as spurious; or * *Fraud analyses*, based on audits of system transaction logs.   The procedures must also provide for *follow-up*, including notification of device owners when business process criteria or fraud analyses indicate spurious submissions as well as disposition of any CORs and signature devices that are involved. | | | |
| **Device Owner Collaboration** | |  | |
| **Business Process Criteria** | |  | |
| **15A** | Does the system use business process criteria to flag submissions as spurious?   * What criteria does the system use? *Examples*: Duplicate reports, off-schedule submissions, deviations from normal content or procedure. | | |
| **15B** | Does the system ever use failed attempts to enter a correct signature device component as a criterion for spurious submission? If it does –   * Under what circumstances is the submission flagged as spurious? | | |
| **Fraud Analyses** | |  | |
| **15C** | Does the system perform fraud analyses of system transaction logs? If so –   * What criteria are used to identify suspicious activity? *Examples*: Unexpected IP addresses, overlapping account sessions. | | |
| **Follow-up** | |  | |
| **15D** | Does the system notify the device owner whenever business process criteria or fraud analyses indicate spurious submissions in his or her name?   * How is the device owner contacted? * What does the notification contain? | | |
| **15E** | What actions are taken with respect to the submissions determined to be spurious?   * Is a COR still created and maintained? * Is the automatic acknowledgement of receipt (under Item 12) still generated? | | |
| **15F** | What actions are taken with respect a signature device that has been used in connection with spurious submissions? | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item 16. Procedures to revoke/reject compromised credentials**  [**Return to Top**](#TOC) | | | | |
| **Requirements:**  A system must have procedures for submissions containing signatures executed with signature devices discovered to be compromised. The procedures must allow the system to both:   * Reject such signatures once the compromise is discovered, and * Determine the status of signatures accepted prior to discovery and maintained in existing CORs.   The system must also have procedures to suspend and restore device owners’ access to their user accounts and their ability to execute e-signatures accepted by the system. | | | | |
| **Signature Rejection** | | |  | |
| **16A** | Once a compromise is discovered, how long does it take the system to suspend acceptance of signatures executed with the device?   * Is the suspension temporary, or is it a permanent revocation of the device?   + If it is temporary, under what circumstances would it be lifted? | | | |
| **16B** | What processes does the system use to suspend acceptance of the signatures? Does the system:   * Suspend recognition of the signature device?   + Are all components suspended, or only the ones discovered to be compromised? * Lock the associated user account? * Close the associated user account? | | | |
| **16C** | How is the device owner notified of these actions? | | | |
| **Signatures in Existing CORs** | | |  | |
| **16D** | When a compromise is discovered, does the system attempt to determine how long the device was compromised?   * If it does, are all the CORs for submissions during the period of compromise flagged as spurious, or is the identified signer asked to determine which are authentic and which are spurious?   + Is the identified signer required to re-sign/certify the submissions he or she determines to be authentic? * If it does not –   + Are any of the CORs containing signatures executed with the device flagged as spurious?     - Is the identified signer asked to determine which CORs are authentic and which are spurious?   + Is the identified signer required to re-sign/certify any of the submissions? | | | |
| **16E** | What does the system do with CORs flagged as spurious?   * If they are retained, do they continue to be available for review by the submitter/signer? | | | |
| **Restoring User Accounts** | | |  | |
| **16F** | When a device is revoked, is the owner always provided with a new device?   * If not, how does the system determine whether to provide a new device? | | | |
| **16G** | How is the new device provided?   * Does the system use the procedures with which the original device was provided (as described under Item 3)? * If there are different procedures –   + What are they?   + How do they ensure that the new device is protected from compromise? | | | |
| **16H** | If the owner’s user account was locked or closed, what are the procedures for unlocking or reopening it?   * How does the system verify the identity of owner, to ensure that access to the account is provided only to the original registrant? | | | |
| **Item 17. Confirmation of signature binding to document content**  [**Return to Top**](#TOC) | | | | |
| **Requirements:**  This requirement applies only where a signer executes a digital signature with respect to an e-document’s content at his or her computer, prior to submission. Digital signature execution involves calculating a hash value for the e-document content and then using a private key to encrypt the hash value. The encrypted hash value is the digital signature.  Once the submission is received, the signature must be validated in three steps:   * Decrypting the signature with the public key that is paired with the private key used to encrypt the document hash; * Calculating a new hash value of the e-document content that was sent; and * Comparing the decrypted hash with the newly calculated hash.   If the signature is valid, the two hash values should be identical. Validity demonstrates that:   * The signature was created with the private key paired with the public key used to decrypt it, and * The document content is unchanged since the time the digital signature was executed. | | | | |
| **Cases:**  There are two cases, depending on the purpose of the digital signatures.   * The signatures serve as e-signatures under CROMERR, satisfying all legal requirements for signatures on submitted documents.   + GO TO **Signature Validation**. * The signatures do not serve as e-signatures under CROMERR, but only provide for the binding of some other signature artifact (such as a PIN plus challenge-question/answer) to the document content.   + GO TO **Signature Binding**. | | | | |
| **Signature Validation** | | |  | |
| **17A** | | Is the public key used to validate the digital signature associated with a PKI certificate?   * If it is, how does the system access the public key that belongs to the identified signer?   + Does the system maintain this key on file, or does it have to interact with an external certificate provider? * If it is not –   + What is the source of the private/public key pair?   + How does the system determine that the public key belongs to the identified signer?   + How is the public key protected from tampering or deletion? | | |
| **17B** | | When are the three signature validation steps performed?   * Does the system include the validation results in the COR?   + If not, how are the results logged? * Are identified signers notified of the validation results?   + How are they notified? | | |
| **17C** | | What actions does the system take if the validation fails? | | |
|  | | **NEXT Copy of Record** |
| **Signature Binding** | | |  | |
| **17D** | | What is the source of the private/public key pair used to execute and validate the digital signature?   * How is the private key made available to the submitter/signer? * How is the public key protected from tampering or deletion? | | |
| **17E** | | When are the three signature validation steps performed?   * Does the system include the validation results in the COR?   + If not, how are the results logged? * Are identified signers notified of the validation results?   + How are they notified? | | |
| **17F** | | What actions does the system take if the validation fails? | | |

|  |  |  |
| --- | --- | --- |
| **Copy of Record**  [**Return to Top**](#TOC) | | |
| In all cases, the system must be demonstrate that it:   * Creates CORs that provide a “true and correct copy” of the document received and contain all the required elements – including all e-signatures associated with the submission in a way that protects associated e-signature devices from compromise (Item 18); * Makes CORs available to agency program and enforcement staff as and when they are needed (Item 19); and * Maintains the CORs in a way that protects their integrity and ensures that they remain available for as long as program and regulations require (Item 20). | | |
| **CROMERR Terms**  compromised – an electronic signature device is *compromised* if the code or mechanism is available for use by any other person than the individual uniquely entitled to use it.  copy of record (COR) *–* 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.  electronic signature (e-signature) – any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic document bears or has on it an electronic signature where it includes or has logically associated with it such information.  electronic signature device (e-signature device) *–* 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. | | |
| **Item 18. Creation of copy of record (See 18a through 18e)**  [**Return to Top**](#TOC) | | |
| **18a. True and correct copy of document received** | | |
| **Requirements:**  For a COR to be a “true and correct copy” of the document received the system must address both:   * *COR Creation* – ensuring that the COR as the system creates it accurately represents the document received; and * *COR Integrity* – ensuring that the COR is maintained with sufficient security to protect it from tampering or deletion. | | |
| **Cases:**   * Checklist describes system that receives only submissions without signatures.   + GO TO **CORIntegrity**. * Checklist describes system that receives signed submissions, so *COR Integrity* issues are addressed under Item 5 (see questions 5H – 5K).   + GO TO **COR Creation**. | | |
|  | |  |
| **COR Integrity** | |  |
| **COR Creation** | |  |
| **18aA** | Does the COR maintain the submission content in exactly the same format in which it was received? If not –   * What processing steps does the content undergo when the COR is created? * Does the processing change any of the submission’s content? * Does the system record any and all changes to the submission content as it is processed?   + How are the changes recorded?   + How is the record of changes (or chain of custody) secured?     - Is the record maintained as a part of the COR?     - Is it maintain for as long as the COR is maintained? | |
| **18b. Inclusion of electronic signatures (e-signature cases only)** | | |
| **Requirements:**  The COR is required to contain any e-signatures executed with respect to the submission. | | |
| **18bA** | Does the COR include all e-signatures executed with respect to the submission content? | |
| **18bB** | In what form or format are the e-signatures included?   * Where the e-signature includes a token of a secret code (such as a PIN) or private information (such as an answer to a challenge-question), how does the system protect these signature device components from compromise when the COR is viewed?   + For example, are they included only in an encrypted format?     - If so, what kind of encryption is used?     - If not, what other measures are taken to prevent signature device compromise? | |
| **18c. Inclusion of date and time of receipt** | | |
| **Requirements:**  The COR must include the date and time of the submission’s receipt by the system. | | |
| **18cA** | Does the COR include the date and time of the submission’s receipt by the system? | |
| **18cB** | How does the system ensure that this date and time cannot be deleted or tampered with while the COR is being maintained? | |

|  |  |  |  |
| --- | --- | --- | --- |
| **18d. Inclusion of other information necessary to record meaning of document** | | | |
| **Requirements:**  The COR must include information necessary to understanding the meaning of the submission’s content and any e-signatures it contains.   * *For all submissions*, such information includes:   + Labels – such as field labels – for data element values, and   + Explanation or formatting that indicates how data elements are related. * *For submission with e-signatures*, such information also includes:   + The identity of the signer,   + The certification language and warnings associated with the e-signatures, and   The format in which the document content was available for review prior to signing. | | | |
| **All Submissions** | | |  |
| **18dA** | Does the COR include labels for submission data element values?   * Are these included for any submission attachments? | | |
| **18dB** | Does the COR include any information necessary to understand how submission data elements are related to each other?   * Are these included for any submission attachments? | | |
| **18dC** | Does the COR include the certification and warning statements that were presented to the user at the time of signing? If not, how does the system demonstrate what warnings were provided and that these warnings have not changed since the time of signature? | | |
| **18dD** | What other information does the COR include that is needed to understand data elements in the submission and any attachments? | | |
| **Submissions with e-Signatures** | |  | |
| **18dE** | Does the COR include information identifying the signer for each e-signature it contains?   * In the case of digital signatures, does the information identifying the signer include references to PKI certificates? | | |
| **18dF** | If the signature includes the answer to a challenge-question, does the COR include the question answered?  Note to Reviewers: Reviewers will assume this is not included unless the CROMERR application indicates otherwise. | | |
| **18dG** | Does the COR include enough information about the format in which the document was available for signer review (see Item 6) to indicate how the content appeared to the signer? *Example*: Where the document was in an XML format, the COR may include the XML schema or style sheet that the system used to display the content on-screen.   * Does the COR include the same information about any submission attachments? * How does the system ensure that this formatting information cannot be deleted or tampered with while the COR is being maintained? | | |
| **18e. Ability to be viewed in human-readable format** | | | |
| **Requirements:**  The system must provide a way to view the COR in a human-readable format. | | | |
| **18eA** | If the COR is maintained in a human-readable format, what is that format? | | |
| **18eB** | If the COR is not maintained in a human-readable format, then –   * In what human-readable format is it made available? * How is it converted into this format? | | |
| **Item 19. Timely availability of copy of record as needed**  [**Return to Top**](#TOC) | | | |
| **Requirements:**  The system must make CORs available to agency program and enforcement staff, as and when they are needed. | | | |
| **19A** | Are CORs of submissions available to agency staff as soon as the submissions are received? If not –   * When do they become available? | | |
| **19B** | Are CORs available to agency staff on-line, or from an on-line site as downloads? If they are not available on-line or as downloads –   * How are CORs obtained? * How long does it take to receive a COR once it has been requested? | | |
| **19C** | Can the system be searched on-line for CORs?   * If it can be searched, what are the search parameters? * If it cannot be searched, how do agency staff locate individual CORs? | | |

|  |  |  |
| --- | --- | --- |
| **Item 20. Maintenance of copy of record**  [**Return to Top**](#TOC) | | |
| **Requirements:**  CORs must be maintained for as long as underlying regulations require their retention, in a way that both protects them from destruction and preserves them as “true and correct” copies of the electronic documents received by the system. To meet COR maintenance requirements the system must provide for:   * *Basic file maintenance*, * *System security*, and * *Record integrity*.   In cases where the required COR retention period exceeds the anticipated life of the current file management infrastructure, the system must also provide for:  COR file migration. | | |
| **Basic File Maintenance** | |  |
| **20A** | Are COR files backed-up?   * What is the back-up schedule?   + Are all records included in every routine back-up, or only those that are new or have undergone changes since the last back-up? * How long are file back-ups maintained? * How are file back-ups protected from tampering or destruction?   + Are they maintained off-site, in a secure location?   + Who has access to the file back-ups?   + How is access controlled? | |
| **20B** | Do the back-up provisions for COR files include the system logs that record COR access and any COR changes?   * If not, what are the back-up provisions for these system logs? | |
| **System Security** | |  |
| **20C** | How are system components, such as the system servers, secured against unauthorized physical access?   * Are these components kept in a locked area? * Who is given access to these components? | |
| **20D** | Does the system include intrusion detection, virus detection, a firewall, and other security? | |
| **Record Integrity** | |  |
| **20E** | Is it possible for system or database administrators, or other agency staff, to change, delete, replace or add a COR? If it is –   * How many staff have this ability? * Are these staff subject to background checks? * Do they sign rules of behavior? | |
| **20F** | Does the system maintain logs of changes to COR files? If it does –   * What triggers a log entry and what data are recorded? * How are log entries protected from alteration and deletion?   + Can system or database administrators, or other agency staff, change, delete, or add log entries?   + How is the log protected from unauthorized changes? * How long are logged entries maintained? | |
| **COR File Migration** | |  |
| **20G** | How long are CORs maintained by the system?   * Does this meet the underlying regulatory requirements for COR retention? | |