|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Item** | Attachment 2 – CDX Registration Maintenance Rules of Behavior Release 1.0.doc  Attachment 3 – RegMain Procedures 12-7-2005.pdf  Attachment 5B - CDX Sample Electronic Signature Agreement.docx  Attachment 6 – Electronic Signature Process.pptx  Attachment 7 – Sample of Review and Confirmation dialogs.doc  Attachment 7B – CDX Registration Electronic Choice Dialogs.pptx  Attachment 9 – CDX Separation of Duties Guide  Attachment 11 - 20-5-1 Questions.doc  Attachment 12 – 20-5-1 e-Signature Registration Process V2.ppt  Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt  Attachment 15 – Content of X.509 Certificate.ppt  Attachment 16 – Electronic (LexisNexis) Identity Proofing Criteria.docx  Attachment 17 – Third Party ID Proofing 5.doc  Attachment 18 – Paper ESA 5.doc  Attachment 19 – CDX Sample Electronic Signature Agreement (paperless ESA).docx  Attachment 20 – Paperless ESA 5.doc Paperless Minimum Validation.docx |

|  |  |
| --- | --- |
| **Registration (e-signature cases only)** | |
| **1. Identity-proofing of registrant** | |
|  | **Business Practices:**  OVERVIEW  **General:** The Central Data Exchange (CDX) identity-proofing procedures are part of the CDX registration process for individuals who will execute e-signatures on reports submitted to the system.  In registering with CDX, an individual specifies the reports for which s/he will execute e-signatures, and s/he is assigned a UserID-password “credential” for this purpose. In conformance with CROMERR requirements for priority reports, identity-proofing of this individual must be completed before CDX will accept an e-signature executed with the assigned credential.  When first entering CDX, registrants are required to read, and accept a CDX warning notice, a privacy statement, and terms and conditions for choosing and protecting the CDX UserID-password that will be tied to the identity-proofing process. The terms and conditions include notifying CDX support staff where changes in duties may require account termination and where the UserID-password may have been compromised.  **Registration Options:** CDX supports two types of registration processes:   1. “Open” registration and 2. “Closed” registration.   **Identity-proofing Options:** CDX supports two approaches to identity-proofing for first-time registrants, both of which are available for either open or closed registration and meet the requirements for e-signatures on priority reports:   1. “Paper-based” approach and 2. “Real time” approach.   **Identity-proofing *Re-Use* Options:** Once the initial registration/identity-proofing process is competed, the individual can register with CDX to use this assigned credential to e-sign additional reports. In such cases:   1. No additional identity-proofing will be required **if** (a) the program receiving the report participates in identity-proofing re-use and (b) does not require more stringent identity-proofing than the original. 2. Otherwise, the registrant will be required to undergo additional identity-proofing.   OPEN REGISTRATION  Under open registration, a new registrant initiates registration by entering CDX to input personally identifying information, including: Name Title, First Name, Middle Initial, Last Name, Name Suffix, Email Address, Street Address, City, State, Zip Code, and Daytime Phone Number.. The registrant then creates a UserID and a complex password (as specified under Checklist Item 3). This UserID-password combination will serve as the registrant’s “credential” for purposes of executing e-signatures.  The registrant receives a confirmation of registration sent to their email address. The confirmation email includes a unique hash key hyperlink which the registrant uses to return to CDX, where they are prompted to choose either paper-based or real time identity-proofing and then to follow the procedures for completing the process.  CLOSED REGISTRATION  Closed registration is limited to individuals who have been identified by the program office receiving the report to be submitted through CDX.  The closed registration process is identical to the open registration process, except that:   * Registrants must use a CDX-generated Customer Retrieval Key (CRK) to initially access CDX for registration; * The registration input screens are pre-populated with information that EPA already has available, which the registrant may edit; * As in open registration, registrants create their UserID-password combination, and receive a confirmation of registration via email that contains the unique hash key hyperlink.   **CRK Issuance Options:** CDX Help Desk support staff generate the CRKs and then:   1. They distribute them directly to registrants who have been identified by the program office; they do this either: (a) by phone, (b) via USPS, or (c) using a combination of email and phone. 2. Alternatively, they deliver the CRKs to the program office, who distribute them to registrants as follows: ***<Insert program-specific details>***.   PAPER-BASED IDENTITY-PROOFING: **See checklist item 1b-alt**  REAL TIME IDENTITY-PROOFING: **See checklist item 1b**  IDENTITY-PROOFING RE-USE  Registrants who are eligible for identity-proofing re-use automatically skip the step of choosing an identity-proofing option and are prompted to sign a CDX electronic ESA (see checklist item #4). |
|  |
| **System Functions:**  For all registration and identity-proofing services, CDX supports access from any World Wide Web Consortium (W3C) open standard web browser.  OPEN REGISTRATION  Service begins with a warning notice, privacy statement, terms and conditions confirmation and logging in support of FISMA security plan requirements specified by NIST 800-18 consistent with minimum security requirements NIST 800-53.  System generates and distributes email confirmation containing unique hash key hyperlink using National Institute of Standards and Technology (NIST) cryptography certified as compliant with Federal Information Processing Standard (FIPS) 142. Successful use of hyperlink allows the registrant to proceed to the choice of an identity-proofing option, as described under the Open Registration Business Practices.  CLOSED REGISTRATION  The CDX system pre-populates the CDX system’s registration tables with the user information provided by the program office. For each prospective registrant, the CDX system then generates a unique, cryptographically hashed Customer Retrieval Key (CRK) to serve as a one-time-only password. When sponsored registrants receive their CRKs, they use a special CDX URL and their CRKs to access their pre-populated CDX registration web pages from their browsers, and they then complete their registration.  PAPER-BASED IDENTITY-PROOFING: **See checklist item 1b-alt**  REAL TIME IDENTITY-PROOFING: **See checklist item 1b**  IDENTITY-PROOFING RE-USE  Registrants who have already undergone CDX identity-proofing are automatically identified through authentication of their CDX UserID-password credential. Credentials are electronically cross-checked with identity-proofing records to determine whether minimum identity-proofing requirements have already been met. |
| **Supporting Documentation (list attachments):**   * Attachment 7B – CDX Registration Electronic Choice Dialogs.pptx * Attachment 18 – Paper ESA 5.doc * Attachment 19 – EPA Paperless ESA.doc |

|  |  |
| --- | --- |
| **1a. (priority reports only) Identity-proofing *before* accepting e-signatures** | |
|  | **Business Practices:**  See Item 1. |
| **System Functions:**  See Item 1. |
| **Supporting Documentation (list attachments):** |
| **1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)** | |
| **1bi. (priority reports only) Verification by attestation of disinterested individuals** | |
|  | **Business Practices:**  CDX offers registrants the option of real time on-line electronic identity-proofing through a third party service provided by LexisNexis. The procedure is the following:   1. For registrants who choose the real time option, a new browser session opens at a LexisNexis web location, which displays a notice informing them that validation information will be returned to US EPA. 2. Simultaneously, CDX sends registration information and a unique transaction Id to LexisNexis, electronically signed and with the CDX certificate. 3. The LexisNexis site asks the registrant to enter information items not provided to CDX, including the last 4 digits of SSN, date of birth, home address, home phone number and, optionally, a Federal Employer Identification Number (FEIN). 4. Given these additional information items, LexisNexis uses the following criteria to verify the identity of the registrant, with the caveat that verification may be rejected if certain risk factors are identified (see Attachment 16 – Electronic (LexisNexis) Identity Proofing Criteria.docx):  * Exact match for Full **or** Last Name **AND** * Exact match for Date of Birth (DOB) **AND** * Exact match for last 4-digits of Social Security Number (SSN4) **AND** * Accurate Home address **or** Exact match for Home Phone number  1. With the registrant’s permission, validation information is returned to US EPA; the LexisNexis browser session closes, and the registrant is returned to the CDX web page from which the LexisNexis session opened. (CDX maintains the validation information for at least 5 years after all CROMERR roles are inactive unless otherwise indicated by the program office.) If the registrant refuses permission to return the validation information to US EPA, the real-time identity-proofing fails; CDX then generates a paper subscriber agreement form for the registrant to download and continues with the paper-based identity-proofing process. |
| **System Functions:**  LexisNexis assigns scores and returns results to CDX in one transaction including input hashed with  FIPS-certified cryptography. The input has sent to EPA includes:  a hash of the following input is returned to CDX:   * Exact match for Full **or** Last Name **AND** * Exact match for Date of Birth (DOB) **AND** * Exact match for last 4-digits of Social Security Number (SSN4) **AND** * Exact match for full 9-digits of SSN (SSN9) **AND** * Accurate Home address **or** Exact match for Home Phone number.   US EPA uses assigned scores returned by LexisNexis to determine the assurance level of the registrant’s identity-proofing.  The basis for a successful registrant identity proofing determination is an exact match on the 5 inputs listed above under paragraph d. bullets. |
| **Supporting Documentation (list attachments):**   * Attachment 16 – Electronic (LexisNexis) Identity Proofing Criteria.docx * Attachment 17 – Third Party ID Proofing 5.doc |
| **1bii. (priority reports only) Information or objects of independent origin** | |
|  | **Business Practices:** See Item 1bi: The LexisNexis site asks the registrant to enter information items not provided to CDX, including the last 4 digits of SSN, date of birth, home address, home phone number and, optionally, a Federal Employer Identification Number (FEIN). |
| **System Functions:**  See Item 1. |
| **Supporting Documentation (list attachments):** |
| **1b-alt. (priority reports only) Subscriber agreement alternative** | |
|  | **Business Practices:**  The CDX paper-based identity-proofing approach is based on collecting a “subscriber agreement” from the registrant under CROMERR section 3.2000(b)(5)(vii)(C). A subscriber agreement is a CROMERR electronic signature agreement (ESA) executed on paper with the registrant’s handwritten signature. The procedure is the following:   1. When the registration process presents the registrant with the two identity-proofing options, s/he chooses the paper-based option. 2. CDX then generates the paper subscriber agreement form, for the registrant to download. A subscriber agreement form contains a unique CDX cryptographic transaction ID which CDX logs to associate the paper form with the registrant’s UserID; it also contains information identifying the registrant and the organization affiliation, including the registrant’s email address and his/her organization name and address. 3. Registrant is placed in a “pending” state until the subscriber agreement is returned to EPA and verified for completeness. 4. The registrant signs the subscriber agreement with a handwritten signature. 5. **Return Options:** Registrant returns subscriber agreement via USPS either (1) to the CDX Help Desk, or (2) to a Registration Maintenance Account Manager (RMAM) delegated by the program office. 6. **Processing Options:** Depending on whether the CDX Help Desk or an RMAM receives the subscriber agreement, either (1) or (2) occurs:    1. CDX Help Desk performs the following steps:       * Verifies that the subscriber agreement has been filled out and signed;       * Validates the information on the subscriber agreement by making telephone contact with the registrant’s authorizing official/employer to confirm business employment and submitter authorization;       * Activates the registrant’s account, and notifies the registrant via email. (Registrant is also notified by email in case the subscriber agreement is deficient and the account is not activated.)   2. RMAM performs the following steps: ***<Insert program-specific details>***   1. **Maintenance Options:** Depending on whether the CDX Help Desk or an RMAM receives the subscriber agreement, either (1) or (2) occurs:    1. CDX Help Desk:       * Stores the received subscriber agreement in a paper-based filing system, in a badge accessible room;       * Retains subscriber agreements for all signing credentials issued on behalf of CDX for a minimum of five years after signature device deactivation.    2. RMAM performs the following steps: ***<Insert program-specific details>*** |
| **System Functions:**  The CDX system presents each user choosing the paper-based option with a web-based link to  download or print the subscriber agreement during the registration process. CDX pre-populates  the agreement with user information obtained in the registration process, including the items listed  under step b. of the procedure described above under “Business Practices”. Before the user can  exit this screen, they are presented with instructions on how to complete the agreement and are told  of the follow-on actions to be taken upon receipt of the agreement by the Program Office or CDX  Help Desk. The user signifies their understanding of these instructions/processing actions by  clicking on the “Finish” button presented. |
| **Supporting Documentation (list attachments):**   * Attachment 2 – CDX Registration Maintenance Rules of Behavior Release 1.0.doc * Attachment 3 – RegMain Procedures 12-7-2005.pdf * Attachment 5B - CDX Sample Electronic Signature Agreement.docx |

|  |  |
| --- | --- |
| **2.** **Determination of registrant's signing authority** | |
|  | **Business Practices:**  There are four options for determining the registrant’s signing authority:   1. A “paper-based” approach carried out by the program office (PO). 2. A “paper-based” approach carried out by CDX, under PO direction. 3. A “paperless” approach shared between the PO and CDX. 4. A “real-time” electronic approach, carried out by CDX.   PO PAPER-BASED APPROACH  The approach generally requires:   * Submission of a sponsor letter to a Registration Maintenance Account Manager (RMAM) delegated by the PO from an official in the registrant’s organization in a position to attest to the registrant’s authority to sign/certify the report(s) in question on behalf of that organization, signed by the official with a handwritten signature. The letter must meet the following requirements: ***<Insert program-specific details>*** * RMAM verification of information in the sponsor letter before CDX activates the user’s account, using the following procedures and criteria for authorization: ***<Insert program-specific details>*** * RMAM retention of the sponsor letter in a secure, paper-based filing system for at least 5 years after being notified of the registrant’s departure from the sponsoring organization by an official of that organization, using the following measures to secure the files: ***<Insert program-specific details>***   The delegated CDX user registration authority (RMAM) must read and acknowledge the CDX Registration Maintenance Rules of Behavior document (see attachment 2) prior to being granted the privileges needed to authorize user access to their CDX-based system. The CDX Help Desk establishes RMAM accounts per the procedures/guidelines noted in the *CDX Registration Maintenance Account Manager (RMAM) Creation Procedures* (see attachment 3)*.*  The CDX Help Desk shall require each POC/RMAM to mail a copy of the CDX “Rules of Behavior” acknowledgement statement to the CDX Reporting Center within thirty days of their sponsorship. The POC/RMAM will be granted access after receiving the acknowledgement statement.  The RMAM’s CDX Registration Maintenance Rules of Behavior acknowledgement is stored in a paper-based filing system. The CDX Reporting Center currently retains the CDX “Rules of Behavior” acknowledgement for a minimum of five years after RMAM account/role deactivation.  CDX/PO PAPER-BASED APPROACH  The approach generally requires:   * Submission of a sponsor letter to the CDX Help Desk from an official in the registrant’s organization in a position to attest to the registrant’s authority to sign/certify the report(s) in question on behalf of that organization, signed by the official with a handwritten signature. The letter must meet the following requirements: ***<Insert program-specific details>*** * CDX Help Desk verification of information in the sponsor letter, using the following PO-specified procedures and criteria for authorization ***<Insert program-specific details>*.** * CDX retention of the sponsor letter in a secure, paper-based filing system for at least 5 years after being notified of the registrant’s departure from the sponsoring organization by an official of that organization.   CDX/PO PAPERLESS APPROACH  The approach generally requires:   * Submission of an electronic sponsor letter to the PO (or RMAM) from an official in the registrant’s organization in a position to attest to the registrant’s authority to sign/certify the report(s) in question on behalf of that organization, signed by the official with a CDX signature credential for which the official as registered with CDX.The letter must meet the following requirements:***<Insert program-specific details>*** * RMAM verification of information in the sponsor letter, using the following procedures and criteria for authorization: ***<Insert program-specific details>*** * CDX retention of the electronic sponsor letter as a copy of record (see checklist item#9a) for at least 5 years after being notified of the registrant’s departure from the sponsoring organization by an official of that organization.   ELECTRONIC CDX APPROACH  This approach is available to registrants who choose the real-time identity-proofing option (See checklist item#1).  LexisNexis verifies the registrant’s identity based on such registrant-provided data elements as name, SSN (last four digits), phone number, while CDX requires the identified user sign specific ESA language attesting that the Certifier has the authority to enter into this agreement to sign and submit reports on behalf of the regulated entity and there are significant penalties for submitting false information, including the possibility of fine and imprisonment.  There are two (2) scenarios for this delegation model:  **Scenario 1: Responsible Official Designates/Sponsors Certifier (RO Initiated Event)**  ROs must first complete CDX registration process, selecting “official” role, identifying data flow(s), completing Third Party Identity Proofing option using LexisNexis Instant ID service, and electronically signing an ESA that includes attestation that registrant is the RO for the regulated entity. (RO can also choose the ESA alternative approach for identity proofing; ESA could include RO attestation.) Once RO completes registration process and is activated by CDX, the RO may designate or “sponsor” Certifiers. To designate/sponsor a Certifier(s) the RO logs-in to CDX, selects RO Sponsorship Tool, identifies data flow(s), and enters email address of Certifier(s). CDX looks up the email address to see if Certifier has an existing CDX user account. If Certifier has an existing CDX account, CDX sends a message to Certifier’s email address, as well as RO’s CDX In-Box and email address. Message contains link to CDX and requests Certifier to accept RO’s invitation for sponsorship and agree to share their registration information with RO. (This step is necessary for PII purposes.) If Certifier accepts RO’s sponsorship, CDX sends message to RO’s CDX In-Box and email address, with link. RO can then view Certifier’s registration information, and generate and electronically sign Sponsor Agreement. CDX then sends message to Certifier’s CDX In-Box and email address, with link to Subscriber Agreement. Certifier accepts and signs agreement. Once signed, CDX activates Certifier’s role for data flow(s) and sends a message to the Certifier email address. If the Certifier does not have an existing CDX account, CDX sends a message to the Certifier’s email address, with a link to CDX registration. The Certifier must first register with CDX, and then complete the CDX identity proofing process and signing ESA after RO logs in to CDX to electronically sign the Sponsor provision in ESA.  **Scenario 2: Certifier Requests Designation/Sponsorship by Responsible Official (Certifier Initiated Event)**  Certifier registers with CDX for first-time or, if registered CDX user, to add additional data flow(s), and provides email address of RO. CDX looks up the email address to see if the RO has an existing CDX account. If the RO has an existing account, then CDX sends a message containing a link to the RO’s email address, requesting that the RO approve or deny the Certifier’s request for sponsorship. To approve sponsorship, the RO electronically signs using his/her CDX e-signature device the Sponsor provision in the Certifier’s ESA, attesting that the Certifier is authorized to sign and submit reports on behalf of the regulated entity. If the request for sponsorship is denied, the RO must provide the reason for denial, but does not e-sign agreement. If the RO does not have a CDX account, then the CDX message requesting sponsorship can only be sent to RO’s email address. The RO must first complete the CDX registration process, using the Third Party identity proofing option, where the ESA includes attestation that the individual is the RO for the regulated entity. Once the RO is registered, RO can then approve or deny Certifier’s Request for Sponsorship. If RO approves, CDX activates the Certifier’s account for data flow(s), after Certifier signs Subscriber Agreement, and sends message to both the Certifier and RO CDX In-Box and email address, notifying that the Certifier is activated and can sign and submit documents for specific data flow(s). If RO denies request for sponsorship, CDX sends rejection message to both the Certifier and RO CDX In-Box and email address. |
| **System Functions:**  During the CDX User Registration or Profile Update processes, the CDX system provides the necessary instructions/forms and prompts the prospective user to complete and mail evidence of signatory authorization to the PO or CDX Help Desk, or provides the link to LexisNexis verification of organizational affiliation. These steps are performed through a series of web-based dialog screens.  CDX employs an application role-based authorization system. By default, the creation of a CDX account does not grant the user any rights or privileges for e-signature or PKI applications, thus prohibiting them from making signed data submissions until the processes of identity-proofing and determination of authorization are completed.  The CDX system provides a web-based mechanism (called Registration Maintenance) for a delegated CDX user registration authority (known as RMAMs) or the CDX Help Desk to grant, deny, or revoke application access to prospective users after determination of the user’s signatory authority (see Attachment 3 for a description of this procedure). This authorization action (and the ID of the authorizing RMAM) is recorded by the CDX system and an approval/disapproval notification sent to the prospective user and other associated RMAMs. Access to the Registration Maintenance function is strictly controlled through the use of User ID/password credentials. |
| **Supporting Documentation (list attachments):**   * Attachment 2 – CDX Registration Maintenance Rules of Behavior Release 1.0.doc * Attachment 3 – RegMain Procedures 12-7-2005.pdf * Attachment 16 – Electronic (LexisNexis) Identity Proofing Criteria.docx |

|  |  |
| --- | --- |
| **3. Issuance (or registration) of a signing credential in a way that protects it from compromise** | |
|  | **Business Practices:**  CDX signing credentials consist of UserIDs and Passwords, where each UserID for an account holder must be unique, supplemented with answer to preset 20-5-1 Challenge Question.  **Policy:**  Issuance and selection of these credentials are governed by strict policies, which the user must accept and acknowledge prior to being granted any authorized privileges through that account. These policies stipulate that the user:   * Select a password that will not be easily guessed (e.g., names, children's names, birthdays, etc.). * Choose a password that is at least eight characters long and contain a mix of letters and numbers. * Protect the password by not divulging the password to any other individual; not storing it in an unprotected location; and not allowing it to be written into computer scripts for automated login purposes. * Take appropriate actions if they believe their CDX User account has been compromised * Notify the CDX Help Desk within ten working days if their duties change and they no longer need to interact with the CDX on behalf of their organization.   **Link with Identity-Proofing:**  The registration process described under checklist item#1 Business Practices help ensures that the registrant who creates the account UserID and Password is the same individual who subsequently undergoes the identity-proofing process for the account:   1. The registrant provides his/her email address during the session in which s/he creates the account UserID and Password 2. CDX gives the registrant access to an identity-proofing session (real-time or paper-based) only after the registrant uses the hyperlink in a confirmation email sent to the email address provided in step 1. 3. The process in step 2 demonstrates that the registrant who enters the identity-proofing session controls access to the email address provided during the session in which the account UserID and Password was created. 4. In addition, to link the registrant to the subscriber agreement in cases of paper-based identity-proofing, this paper document includes:    * + The registrant’s email address,      + The registrant’s CDX UserID, and      + A unique CDX cryptographic transaction ID which CDX logs to associate the paper form with the registrant’s UserID (see checklist item#1b-alt). |
| **System Functions:**  **General:**  Transaction Security: All user access and information exchange with the CDX system is done over a Secure Socket Layer (SSL) connection between the user’s web browser and the CDX Web/Application Servers. This prevents third parties from being able to decipher/view secrets or other sensitive information being exchanged with CDX during a user’s active web browser session. Negotiation of the version of SSL used for this secure session is controlled through server configuration files. Connection requests from browsers that support only older, lower security versions of SSL (i.e., SSL 1.0 or SSL 2.0) are rejected by CDX.    Secure Identity Management: CDX provides a layered approach to applying security controls in order to maintain the integrity/confidentiality of user Identity Management-related secrets; this approach uses a combination of physical security, personnel security, vendor product security, and CDX application logic security. For example, suspect persons would need to be granted facility access, server room access, OS-level access, and vendor product access to simply view an identity management database table entry. Even with this access, the information they would see would be unusable to them in any meaningful way, as the CDX system applications store only resultant data in these repositories – not the actual input data (i.e., secrets) needed to re-create this result.  **Credential Issuance:**  Users specify their selection of a CDX UserID and Password as part of the general CDX user registration process (see checklist item#1). The UserID and password must each be at least 8 characters long and contain a mixture of letters and numbers. A UserID must be unique within CDX; a password may not be unique. Further, CDX follows EPA guidance for password strength. Passwords must include at least 8 alpha-numeric characters, with at least one upper case and one lower case letter, and at least one numeric character. CDX includes periodic password resets according to Agency requirements. The CDX system enforces password strength requirements and automatically rejects any password that does not meet those requirements.  Upon entry the user’s selected ID is stored in the CDX registration database, and the password is stored in a protected manner as follows:   * UserID and password are encrypted or hashed * The each value is hashed in accordance with Federal Information Processing Standards (FIPS) (e.g., SHA-256)   **Credential Use and Maintenance:**   * Use of the password to authenticate a user is done by comparing the hash value of the current user-entered password with the hash value of the most recent password on file for that user. * Passwords are automatically expired by the CDX system per standard EPA policy. * Users are sent an out-of-band email notifying them of their userid-password being locked along with instructions on how to reset their account. * CDX retains hash of previously created passwords for user in order to prevent password re-use and for e-signature revalidation purposes.   CDX enforces EPA guidance for password strength (e.g., at least 8 alpha-numeric characters, at least one upper case, and at least one numeric and periodic password reset), and passwords are one-way encrypted to resist decryption techniques such as brute force and dictionary attacks. Also, all password resets are logged. Further, password and 20-5-1 answers are stored on separate servers, and only administrators have necessary privileges to access password hashes or 20-5-1 answer hashes and separation of duties assures that administrators have access to only password hashes or 20-5-1 answer hashes but not both.  **Establishment of 20-5-1 Questions/Answers:**  After the completion of the on-line portions of the identity-proofing process (see checklist item#1) and electronic signature agreement process (see checklist item#4), the system displays a list of twenty questions, from which the user selects any five. For each of the five selected questions the user is asked to provide a secret answer.  Each of these answers is independently secured as follows:   * The system retrieves the latest hashes of the user's password * The system concatenates the UserID, question #, user-supplied answer, and latest hash of the user's password * The concatenated value is hashed in accordance with Federal Information Processing Standards (FIPS) (e.g., SHA-256)   **Distinct Security Question Number/Answer Pair for Account Resets:**  At a later date, the user may need to reset their account password or reselect/re-enter 20-5-1 questions/answers. To allow for this, the system also requires that the user specify a special secret question and secret answer that is independent of the 20-5-1 questions/answers. This special secret question/answer helps authenticate the user to the CDX Help Desk or to the system in the case of self-service profile updates. Provision of both the question and answer (along with other identity information) helps confirm that the user is the original registrant for the account. The secret portion of this information is secured as per the account password. All updates to user profile items are secured as indicated above and the user is sent an out-of-band email message notifying them of any account modifications. |
| **Supporting Documentation (list attachments):**   * Attachment 11- 20-5-1 Questions.doc * Attachment 12 – 20-5-1 e-Signature Registration Process V2.ppt * Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt |

|  |  |
| --- | --- |
| **4. Electronic Signature Agreement** | |
|  | **Business Practices:**  There are two options for executing an electronic signature agreement (ESA):   1. The paper-based subscriber agreement approach, and 2. The electronic ESA approach.   PAPER-BASED SUBSCRIBER AGREEMENT  **Process:**   * See the procedures for subscriber agreements described under checklist item#1b-alt, Business Practices. * By affixing their signature a subscriber agreement users explicitly provide their agreement to adhere to the CDX policies, terms, and conditions listed in the agreement.   **Content:**   * A registrants signing the subscriber agreement agrees to the following:   (1) Agree to protect the electronic signature credential, consisting of my Central Data Exchange (CDX) UserID and password, from use by anyone except me. Specifically, I agree to maintain the secrecy of the password; I will not divulge or delegate my user name and password to any other individual; I will not store my password in an unprotected location; and I will not allow my password to be written into computer script to achieve automated login;  (2) Agree to contact the US EPA CDX help desk at 1-888-890-1995 as soon as possible, but no later than 24 hours, after suspecting or determining that my user name and password have become lost, stolen, or otherwise compromised;  (3) Agree to notify CDX within ten working days if my duties change and I no longer need to interact with the CDX on behalf of my organization. I agree to make this notification by notifying the CDX Technical Support staff at 1-888-890-1995 or [helpdesk@epa.gov](mailto:helpdesk@epa.gov);  (4) Understand that I will be informed through my registered electronic mail (e-mail) address whenever my UserID or password have been modified;  (5) Understand that CDX reports the last date my UserID and password were used immediately after successfully logging into CDX;  (6) Understand and agree that I will be held as legally bound, obligated, and responsible for the use of my electronic signature as I would be using my hand-written signature;  (7) Understand that whenever I electronically sign and submit an electronic document to CDX, I will receive an e-mail at my registered e-mail address. This e-mail will inform me that a submission has been made to CDX from my user account and will contain instructions to view information regarding the submission, including my Copy of Record (CoR);  (8) Agree that if I receive an e-mail notification for any activity that I do not believe that I performed, I will notify the CDX Help Desk as soon as possible, but no later than 24 hours, after receipt;  (9) Agree to contact the CDX Help Desk if I do not receive an e-mail notification within 5 business days for any electronically signed submission using my credentials;  (10) Agree to report, within 24 hours of discovery, any evidence of discrepancy between any electronic document I have signed and submitted and what the CDX has received from me by contacting the CDX or service Help Desk;  (11) Agree to notify the EPA if I cease to represent the regulated entity specified above as signatory of that organization’s electronic submissions by contacting the CDX Help Desk as soon as this change in relationship occurs and to sign a surrender certification at that time; and  (12) Agree to retain a copy of this signed agreement as long as I continue to represent the regulated entity specified above as signatory of the company’s electronic submissions.  (13) Certify I have the authority to enter into this Agreement on behalf of the Organization identified above, and I am a signatory authorized to represent that Organization, and I am able to sign and submit reports and other information on behalf of that Organization in the capacity required by statue and/or regulation.  (14) Certify that by signing and submitting this agreement, I have read, understand, and accept the terms and conditions of this electronic signature agreement. I certify under penalty of law that I have personally examined and am familiar with the information submitted in this agreement and I believe that the information is true, accurate and complete. I am aware that there are significant penalties for submitting false information, including the possibility of fine and imprisonment.   * In addition, the subscriber-agreement must contain the following items of registrant-provided information: Company Name, Address/City/State/Zip, Site Name, Signatory Name, Email Address, selected CDX UserID, Date, and Title. The CDX Help Desk will not approve a subscriber agreement that does not contain all of the above items, as this subscriber agreement is used to link the uniquely named/identified individual to their CDX-issued signature credentials. * **Additional Optional Items:** At the Program Office’s request, the ESA also includes: ***<Insert program-specific details>***.   ELECTRONIC ESA  **Process:**   * Electronic ESAs are used either where the registrant has chosen the real-time identity-proofing, or where the registrant executing an ESA in conjunction with identity-proofing re-use (see checklist item#1). * For applications where an Electronic Signature Agreement (ESA) is required, CDX provides each registrant with access to the ESA during the on-line user registration process. * The registrant signs the electronic ESA with his/her CDX-issued signature credentials. * CDX maintains the electronic ESA as a copy of record (see checklist item#9a) for at least 5 years following deactivation of the associated electronic signature tool.   **Content:**   * A registrant signing an electronic ESA agrees to the same 14 items listed above, under the content of the paper-based subscriber agreement. * **Additional Optional Items:** At the Program Office’s request, the electronic ESA also includes: ***<Insert program-specific details>***. |
| **System Functions:**  PAPER-BASED SUBSCRIBER AGREEMENT  See the system functions for subscriber agreements described under the “System Functions” section of checklist item#1b-alt.  ELECTRONIC ESA   * The system pre-populates the ESA with user information obtained in the registration process, including the user-selected CDX UserID. * The system makes the ESA available, on-screen, at the conclusion of the real-time identity-proofing process, or where otherwise appropriate. * The system provides the following procedure for electronically signing the ESA:   + A window opens and provides the registrant an option for electronic ESA.   + The registrant chooses the electronic ESA option by clicking on a button on the screen and is then prompted to establish CDX TRC-approved 20-5-1 secrets, if they do not already have them.   + Once the registrant has established 20-5-1 secrets, s/he will be provided with a human-readable copy of the CDX e-ESA, which s/he eSigns the e-ESA following CDX’s electronic signature process (see checklist item#5).   + CDX electronically signs the CDX registration information and ties it together with a timestamp and the unique transaction ID, which CDX associates with the registrant through his/her UserID. |
| **Supporting Documentation (list attachments):**   * Attachment 5B - CDX Sample Subscriber Agreement (paper ESA).docx * Attachment 19 – CDX Sample Electronic Signature Agreement (paperless ESA).docx * Attachment 21 – CDX Sample Agreement for “Consolidated ESA” |

|  |  |
| --- | --- |
| **5. Binding of signatures to document content** | |
|  | **Business Practices:**  The CDX supported signing method requires the user to enter his/her electronic signature credential, consisting of his/her UserID and password, supplemented by answer to one of 5 preset “20-5-1” Challenge Questions prompted at random. |
| **System Functions:**  During the submission process, users are informed of the implications of their review/certification/signing of submission documents and acknowledge them using the mechanisms described in items 6 and 7. After this acknowledgement, CDX uses an electronic signature tool and prompts the user for their current account password. The password entered by the user during the signing ceremony is one-way encrypted or "hashed". The resulting hash value is then compared with the hash value of the current user password stored in CDX. The agreement of the two hash values validates the Password entered by the user, and ensures that the account owner who originally logged into the session has not walked away from their workstation allowing someone else to perform actions related to the submission or signature process.  Once the Password is validated, the system will randomly choose one of the five questions selected by the user during registration for the 20-5-1 security technique and will request that the user provide the correct response to that question. The answer the user enters is then also one-way encrypted or hashed and compared with the hash value of the answer as originally recorded. The user is allowed three attempts to provide the correct answer. A third failed attempt results in termination of the submission/signing process; in addition, the account is locked, the incident is logged in the CDX audit trail, and an automated e-mail is sent to the email address on file for the account owner stating the account has been disabled due to validation failure. If the hash value of the entered 20-5-1 security question answer matches the hash value stored in CDX, then a *Submit* button appears for the user; and by clicking *Submit* the user signifies their acknowledgment of the penalties for submitting false information, etc.  Once the UserID, Password and answer to the 20-5-1 security question are validated, and the user clicks *Submit,* the actual report is then encrypted and the signature process is completed using a one-time temporary public/private key pair generated on the client workstation, as follows:  CDX uses an electronic signature tool to create a public/private key pair based on X.509 standards (currently 2048bit). The public key from this process is stored in a temporary X.509 signing certificate that also includes current user/session information, and is signed by a CDX server process using a CDX server private certificate. The certificate is temporary in that it is used only for a single signing session, and is not retained on the user’s workstation after the session is completed. The public certificate is, however, retained by CDX and included in the copy of record (COR) for the submission. The temporary X.509 signing certificate includes: the public key of the Submitter’s signature key pair generated during the session, UserID, hash of the password entered during the signing ceremony, 20-5-1 prompted Question Number, hash of the 20-5-1 security question answer, timestamp, and other information from the signing ceremony.  A message digest for the submission document (or documents if multiple documents make up the submission) is created by the CDX electronic signature tool using a detached signature hash algorithm maintained within the detached signature file using Federal standard algorithms (presently contains a SHA-256 algorithm), and then this message digest is encrypted using the user’s private key and the standard method is also maintained within the detached signature (currently includes SHA-256). The temporary X.509 certificate, the document signature (encrypted document message digest), the document digest, and signature methods are packaged in the detached signature file, and uploaded to the CDX server and stored in a COR record with a unique transaction ID. CDX verifies that the certificate issuer signature contained in the temporary x.509 certificate matches the official CDX signing certificate. If the issuer information is incorrect, then the submission is rejected and an e-mail notification to this effect is sent to the registered email address for the submitter with a corresponding message placed into the submitter’s MyCDX in-box. This condition is also noted in the CDX audit logs. |
| **Supporting Documentation (list attachments):**     * Attachment 6 – Electronic Signature Process.pptx * Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt |

|  |  |
| --- | --- |
| **6. Opportunity to review document content** | |
|  | **Business Practices:** |
| **System Functions:**  When the user completes data/metadata entry and/or submission file selection, the CDX system will display a “review and confirm” dialog consisting of one or more pages of read-only information about the prospective submission. This dialog allows the user the opportunity to review all of their submission-related information prior to final submittal.  There are two types of dialogs:   * For simple file uploads, this dialog contains summary information about the submitter’s identity and the to-be-uploaded file; such as full directory path of the file, the file name, file date/time stamp, and file size. * For data entry made via web forms, the system generates a PDF or formatted HTML page containing the submitter identity information and all submission-related data entries made by the user on the data/metadata collection web forms that CDX provided for that purpose. .   For both types of dialog, the user must acknowledge the “review and confirm” dialog(s) by clicking on the SUBMIT button in order to be able to complete their submission. Pressing the BACK or RETURN TO FORM buttons will return the user to the original data entry dialogs where they can correct their data or terminate the submission.  The user’s acknowledgment of the “review and confirm” dialog information (i.e., the SUBMIT button click) will be logged by the system in the CDX audit tables. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **7. Opportunity to review certification statements and warnings** | |
|  | **Business Practices:**  The specific text displayed by the system in the signature certification and warning statement(s) used by an application is specified by the individual EPA Program Offices. |
| **System Functions:**  There are two signing cases: either the submission is signed on-line as a part of a CDX user session, or else the submission may be signed off-line at the user’s workstation.  On-line Signature: Prior to initiating the signature process described in item 5, the system will display a web-based dialog containing a certification/warning statement concerning the proper use of their signing credential, the legal implications of attaching their electronic signature to their submission materials, and an affirmation that the signatory is not aware of any compromise of their signature credential. The user must acknowledge that they have read, understood, and agree with this certification/warning statement by clicking on a check box before the SIGN or SUBMIT button on the dialog will be activated and the submission step completed. The user’s acknowledgment of the certification/warning statement dialog (and/or the click on check box) will be captured in the CDX audit tables.  Certification statements displayed by the CDX system will be program/report-specific, but an example is: “I certify under penalty of law that I have personally examined and am familiar with the information I submitted in this and all attached documents, and that based on my inquiry of those individuals immediately responsible for obtaining the information, I believe that the submitted information is true, accurate, and complete. I am aware that there are significant penalties for submitting false information, including the possibility of fine and imprisonment. “  Off-line Signature: Some submission files may be signed offline, before CDX is accessed for file upload or submittal. In those cases, CDX does not initiate the signature process described in item 5; however, the system does make the user acknowledge a signature certification statement during the submission process, to ensure that the user is apprised of the implications of affixing their electronic signature to the submission document by their offline signing application. The user must acknowledge that they have read, understood, and agree with this certification/warning statement before the SUBMIT button on the dialog will be activated and the submission step completed. The user’s acknowledgment of the certification/warning statement dialog (and/or the click on check box) will be captured in the CDX audit tables. |
| **Supporting Documentation (list attachments):**   * Attachment 7 – Sample of Review and Confirmation dialogs.doc |

|  |  |
| --- | --- |
| **8. Transmission error checking and documentation** | |
|  | **Business Practices:** |
| **System Functions:**  CDX uses only SSL-secured HTTP sessions (HTTPS) for conducting business transactions. CDX Supports SSL v3.0, 128 bits and TLS v1.0 256 bits. These protocols provide for encrypted application messages to be exchanged between Client and Server. As every data record must be successfully decrypted on the server using the negotiated key in order for the connection to remain viable, the integrity of the received data record is ensured. If data is found to be corrupted during transmission (i.e., the Server decryption fails) the protocol automatically retransmits. User transmission failures are logged by the system. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **9. Opportunity to review copy of record** | |
| **9a. Notification that copy of record is available** | |
|  | **Business Practices:**  The Copy of Record (COR) is created when the user completes the submission certification acknowledgement process. All data items that make up the COR are then stored/retained in the CDX archive database tables, which reside on an Oracle database server. Uploaded submission files and any necessary related XSL files are stored in the archive database as binary large object (BLOB) types due to their variable size; BLOB storage allows these files to retain their native formats, which may include text (.TXT), Extensible Markup Language (XML), Portable Document Format (.PDF), Comma-Separated Values (.CSV), Zip data compression format (.ZIP), and Microsoft Word (.DOC). Other COR items are of fixed length and are given the appropriate field type. Each submission file that makes up the submission event is given a unique document ID in the archive, with all such document objects being associated with the same underlying submission transaction ID.  There are CDX CORs for two types of submissions: submission with electronic signatures, un-signed submissions, and encrypted submissions.  Submissions with Electronic Signatures: The COR for CDX in this case consists of:   1. The submission file (or files) – along with the digital signatures and signatory public keys associated with the temporary X.509 certificate described under item #5 of this checklist. 2. A flat or xml header file created by CDX containing submitter identity information and any metadata collected as part of and associated with this submission – along with the digital signatures and signatory public keys associated with the temporary X.509 certificate; Userid and hashed password are included 3. A unique Transaction ID associated with the submission 4. The date/time stamp of submission 5. The temporary X.509 certificates associated with this submission, which are needed to tie the public key to a particular user in cases where the submission includes an electronic signature. 6. An XSL style sheet (to apply against XML submission file(s) or metadata documents) is included if XML-style documents are included as part of, or generated during, the submission process.   Un-signed Submissions: CDX CORs for un-signed submissions omit any user-signature-related data elements. However, CDX will sign the submission file upon receipt, using the private key associated with the CDX system X.509 certificate. Signature information from this signing action will be stored with the user-supplied submission information in the COR in a fashion similar to that employed for user-signed files.  In both cases, users are notified of the availability of their CDX COR using the system functions described below. Specific textual content of the notifications is provided by each sponsoring Program Office; however, certain routine COR items such as UserID, date/time of submission, transaction ID, and the file name(s) of each submission file are included in this message by default.   * Insert any additional Program data elements included in emails: ***<Insert program-specific details>*** |
|  | **System Functions:**  CDX provides each registered user with browser-based access to an individualized messaging In-box function (called MyCDX In-box).  A system message is inserted into the user’s MyCDX In-box for each data submission made through CDX. CDX also delivers these messages as an email notification to the email address on file for the account owner where appropriate.    The MyCDX In-box and email messages contain information on the success/failure of the data submission process, as well as instructions and URL links relevant to the submitted information. Such instructions indicate how to access/browse/download the COR – either from a CDX location or from the back-end Program Office application. The message notification process is template-driven and dynamically configurable in order to allow flow-specific parameters and text items to be included in the message. These included parameters can indicate the UserID, date/time of submission, transaction ID, and the file name of the original submission. |
| **Supporting Documentation (list attachments):** |
| **9b. Creation of copy of record in a human-readable format** | |
|  | **Business Practices:** |
| **System Functions:**  There are three cases, depending on the format in which the submission is received:   1. User-supplied submission input entered via CDX web-based forms: CDX creates an XML-based submission file. A style sheet is then applied to this XML file and it is then “printed” to a PDF. This PDF serves as the COR submission document in a human-readable format. This procedure is used even for those web forms that ordinarily write their data directly to database tables. 2. User-generated files uploaded to CDX: These are maintained and provided back to the submitter in their native format. 3. Submission file received from the user in an encrypted form: Such files can only be decrypted and used by the back-end Program Office system and by the submitter. To decrypt the COR, the submitter is prompted for his/her decryption password. |
| **Supporting Documentation (list attachments):** |
| **9c. Providing the copy of record** | |
|  | **Business Practices:** |
| **System Functions:**  For every submission, the user has two options for accessing/downloading their COR on CDX:   * MyCDX Inbox Option: The MyCDX In-box provides the user with a list of messages related to their submissions. Those messages contain links to the COR along with instructions on how to download and view any COR information. * Transaction History Dialog Option: This option includes search capabilities for users looking for CORs of older submissions. To access this option, users log into CDX to view all data/documents related to their submissions via a transaction history dialog. Users can search by date range and are provided with a list of all COR items that meet that criterion. The default date range is all submissions made during the last five days. Users can view download documents from this dialog.   + If the COR is the original submission document, the document is available as soon as the submitter completes the data submission.   + If part of the COR needs to be "processed and supplied" by a back-end application, the back-end application will submit that portion of the COR to CDX upon completion of processing, and CDX will relate that data item back to the original submission through the transaction ID.   + If any portion of the COR is encrypted for transmission to the back-end application, CDX will rely on that application to re-encrypt the COR and submit that portion of the COR back to CDX for provision to the user. CDX will relate that COR data item back to the original submission through the transaction ID. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **10. Procedures to address submitter/signatory repudiation of a copy of record** | |
|  | **Business Practices:**  Users who wish to dispute their submission of a document corresponding to a COR contact the Program Office (PO). The PO provides users with instructions on the dispute procedures as follows: ***<Insert program-specific details>***.  Users may base their dispute of a submission on one or more of the following four claims:   1. The COR does not accurately represent the content of the corresponding submission. 2. The submission was made with erroneous content. 3. They did not submit any document corresponding to the COR. 4. In the case of electronically signed documents, the signature was executed by someone else using their credential.   The PO responds to such disputes as follows:   * The PO contacts the CDX Help Desk to obtain the submission data and associated metadata, include the date/time of submission, the submitting UserID, the user audit trail log, and any public keys and signature hashes that were stored with the submission. Receipt of a request for assistance from the Program Office would be captured in the CDX Help Desk ticketing system. * The PO uses the information it receives from the CDX Help Desk, along with items from any ESA/Sponsor Letters to establish the identity and authority of the user with respect to the submission they wish to dispute, as follows: ***<Insert program-specific details>*** * If the user dispute is based on Claims 1 and/or 2, the PO assesses these claims as follows: ***<Insert program-specific details>***   + Where the PO determines the appropriate remedy involves revisions of the submission, the PO reports problem to CDX Help Desk and the CDX system provides for submission of revisions to submitted documents in the same manner as the original submission.   + The PO is responsible for establishing, documenting, and following the policy and procedures defined by their program to accurately process the replacement/supplemental submission. * CDX treats these re-submissions as a distinct new COR. In such cases, CDX maintains the original COR and the CORs for all re-submissions; the COR with the most recent date/time stamp is considered the current COR. * If the user dispute is based on Claims 3 and/or 4, the PO assesses these claims as follows: ***<Insert program-specific details>***   + If the PO determines that the user’s signature credential has been compromised (Claim 4), the Office is required to contact the CDX Help Desk and request that the user’s account be locked to prevent additional compromises.   + EPA’s CSIRC is responsible for investigating and assessing all security incidences, including those involving the CDX system. CSIRC: investigates how the account may have become compromised, assesses the extent of the compromise, determines action to be taken, including whether any additional submissions need to be repudiated; and recommends steps to prevent future occurrences. |
| **System Functions:**  For CROMERR-related applications, the system will provide users with access to their transaction history dialog. This function allows the user to browse/search for any potentially suspect submissions and initiate repudiation-related communications with Program Office representatives. The CDX system flags any CORs that have been repudiated by the CDX Help Desk using the CDX Help Desk tool after receiving word from the certifier or the Program. Users are able to view CORs that have been flagged as repudiated in their transaction history dialog. The CDX system provides a web-based mechanism for the CDX Help Desk to lock a user’s account and to revoke or re-issue a signing credential.  . |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **11. Procedures to flag accidental submissions** | |
|  | **Business Practices:**  Users who accidentally submit the wrong file or submit faulty data contact the Program Office (PO). The PO provides users with instructions on corrective procedures as follows: ***<Insert program-specific details>***.  The PO responds to such notifications as follows:   * The PO contacts the CDX Help Desk to obtain the submission data and associated metadata, including the date/time of submission, the submitter’s UserID, the user audit trail log, and any public keys and signature hashes that were stored with the submission. Receipt of a request for assistance from the Program Office would be captured in the CDX Help Desk ticketing system. * The PO uses the information it receives from the CDX Help Desk, along with items from any Subscriber Agreement or ESA and Sponsor Letters to establish the identity and authority of the user with respect to the submission they wish to have corrected, as follows: ***<Insert program-specific details>*** * The PO determines appropriate corrective action, as follows: ***<Insert program-specific details>***   + Where the appropriate action involves revisions of the submission, the CDX system provides for submission of revisions to submitted documents in the same manner as the original submission.   + The PO is responsible for establishing, documenting, and following the policy and procedures defined by their program to accurately process the replacement/supplemental submission.   + CDX treats these re-submissions as a distinct new COR. In such cases, CDX maintains the original COR and the CORs for all re-submissions; the COR with the most recent date/time stamp is considered the current COR.   The CDX system flags CORs of submissions that were submitted “accidentally” or by mistake as rejected; and the system sends a message to the user’s out-of-band account email address and CDX In-Box notifying the user that the submission is rejected. |
| **System Functions:**  The CDX system allows resubmission of data if the user finds an error in the original submission, subject to the PO’s regulations regarding corrections and/or re-submittals.  CDX provides multiple system mechanisms to prevent and identify accidental or erroneous submissions.   1. During data entry or file selection:    1. By validating all user entries on all data entry forms and fields. Field items are checked for conformance with expected data lengths, types, formats, attributes, etc.    2. By validating the necessary inclusion of all dependent data fields.    3. By providing users with the opportunity to interactively browse to select the submission file they intend to submit, instead of asking users to type in the file name and path.    4. By performing simple file validation checks on user-entered or selected file names, such as properly constructed/formatted file names and inclusion of expected file extensions.    5. By automatically providing help to the user in finding the signed versions of their submission file(s) on their file system where necessary. 2. During the submission process:    1. Users are given the opportunity to review the transaction metadata related to submission in a read-only manner prior to being able to submit.    2. Users must confirm all submission actions via a confirm/certify page. 3. Upon/after submission:    1. XML submission files are checked for conformance with schema definition standards and users are notified by email of the location and type of error found.    2. XML submission files are checked for business rule conformance (e.g., State Name abbreviations should follow standard two letter conventions, etc.) and users are notified by email of the location and type of error found.    3. Submission files are subject to validation of proper file types (XML vs. .ZIP), etc. and users are notified by email if errors are found.    4. Submitters receive an email confirmation and MyCDX in-box notification of every submission, even those that are rejected due to processing errors.    5. Processing reports received from back-end systems that are related to a specific submission are e-mailed to the appropriate user and/or placed in their MyCDX In-box.    6. Users can review the CORs of all previous submissions by accessing their MyCDX In-box or their transaction history dialog. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **12. (e-signature cases only) Automatic acknowledgment of submission** | |
|  | **Business Practices:** |
| **System Functions:**  Upon the user’s acknowledgment of the “Confirm” or “Certify” submission dialogs (i.e., clicking on the FINISH or SUBMIT button), the on-line user is shown a simple dialog that confirms that a submission was just completed. The language on this dialog thanks the user for making the submission and gives general information about subsequent actions to be taken by the system – such as what reports will be sent to the user’s MyCDX In-box, the list of other users who will be notified of the submission, etc. Upon closing this dialog, the user is returned either to the submission preparation dialog screen in order to prepare further submissions or to their MyCDX home page.  In addition to the on-line dialog, an acknowledgement notification is automatically sent by the system through an out-of-band e-mail message to the submitter’s registered email address. The notification includes the UserID used in making the submission, the timestamp of the submission, the transaction ID, and other information related to the submission. This notification is also placed in the user’s MyCDX In-box. In cases where the email has been determined to be undeliverable, CDX records this fact in the transaction log and the CDX Help Desk takes follow-up action by telephoning the user or contacting the user through other means. This follow up action is necessary to ensure that the account has not been compromised. If the CDX Help Desk is unable to contact the user, it will follow-up with the regulated entity.  CDX also provides automatic acknowledgements to the user when there are significant changes to the user’s account profile, such as changing the account email address. In cases where a user changes their account email address, the system automatically sends an email to both the new and the old email addresses.  As necessary, CDX is capable of automatically delivering these notification messages to other authorized users, such as a reviewer group or a certification official, as requested. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Signature Validation (e-signature cases only)** | |
| **13. Credential validation (See 13a through 13c)** | |
| **13a. Determination that credential is authentic** | |
|  | **Business Practices:** |
| **System Functions:**  The credential used to create the signature in the e-Signature case is the UserID/Password supplemented with a 20-5-1 question/answer as a second factor. CDX determines that this credential is authentic by verifying that the UserID/Password and question/answer are associated with the user’s registered account profile.  See checklist item#3 for details on how CDX securely issues and protects the Pin/Password.  See checklist item #5 for details on how CDX creates the temporary X.509 certificate. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **13b. Determination of credential ownership** | |
|  | **Business Practices:** |
| **System Functions:**  CDX verifies that the hash value of the UserID/Password entered in executing the user’s e-signature matches the submitter’s CDX UserID/Password hash as stored in the system’s Registration database. If the information does not match then the submission is rejected and an out-of-band e-mail will be sent to the registered users email address for that certificate and a message will be placed into that user’s MyCDX in-box. This condition is also noted in the CDX audit logs.  In cases where user registration included real-time identity-proofing (see checklist item#1b) CDX 3rd Party identity proofing criteria may be re-validated by re-registering the user through the 3rd party and confirming that the same criteria for Hashed Last Name, Hashed SSN 9 digits, Hashed Date of Birth (hashed individually by month/day/year) are the same. Additional hashed values for Street Address, City, State Abbreviation, and Zip Code add evidence for identity tied to copy of record for both the Electronic Signature Agreement (ESA) and subsequent e-Signatures tied to submissions. CDX also has hash of the last 4 digits of the SSN which can be used as well if there is some discrepancy. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **13c. Determination that credential is not compromised** | |
|  | **Business Practices:**  None |
| **System Functions:**  For the e-Signature cases, the signing instrument is the password used in conjunction with the UserID. However, in executing an electronic signature the password-plus-UserID is used together with a 20-5-1 security question/answer as a second factor. The answers to the 20-5-1 security questions are secrets known only to the user, which they are likely to know from memory based on their personal history. Thus, the fact that a randomly selected 20-5-1 security question has been correctly answered provides independent evidence that the individual answering the question and entering the password is the registered account owner, and thus that the password remains uncompromised and within the account owner’s exclusive control.  See the discussion in item #3 for details on how the password and 20-5-1 security question/answer are protected from disclosure. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **14. Signatory authorization** | |
|  | **Business Practices:** |
| **System Functions:**  CDX makes use of role-based user access controls. Only those users who have been granted a signatory role for an application per Item 1b of this checklist are allowed access to the web-based dialogs and web services needed to perform the associated signing actions. All other users are denied access to those functions through a combination of programmatic and system level access control mechanisms. For example, every CDX Java or Active Server Page contains code that validates the user’s current logged-in session/account information against the specific CDX policy needed to display that web page. If the user does not have the appropriate CDX policy, the server will display a “403 - Access Forbidden” page.  See checklist item#2 for details on how this role-based access is granted by the CDX Help Desk or Program Office RMAM. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **15. Procedures to flag spurious credential use** | |
|  | **Business Practices:**  The CDX Electronic Signature Agreement (ESA) requires the user to notify the CDX Help Desk or the sponsoring Program Office if they receive notification of a submission that they did not make. To ensure that the user is able to detect such incidents, some information provided during the user’s registration process cannot be changed on-line as means of preventing spurious changes to account information by someone who may have subsequently gained access to that account. For example, changing the user’s registered email address requires that user contact the CDX Help Desk and verify their identity as the registered CDX account owner by providing specific information (e.g., user’s organization, organization address, and user’s phone number) and successfully answering a pre-established Security Question that was setup during registration to verify identity for account profile changes. Also, CDX sends a message notifying the user of any account profile changes to both the user’s registered out-of-band email address and CDX In-Box. If the user changes their registered out-of-band email address, CDX sends the email message to both the new and the old account email addresses; as well as the user’s CDX In-Box. |
| **System Functions:**  The CDX security engineers perform a weekly review of all security-related log files on the system (audit logs, etc.) and follow a documented security incident response procedure when any suspicious activities are noted, such as multiple failed login attempts, certificate validation failures, etc. This response procedure ensures that both CDX and Program Office authorities are notified in the event of a security issue.  In addition, during the e-Signature document signing procedure, the user is prompted to supply their user account password and answer to one of the “20-5-1” challenge questions selected at random by the system. A failure to enter either value correctly at this point will prevent the signature action from being completed. Three successive failures will result in an account lock-out, which will automatically trigger a notification sent both to the registered email address for that UserID and to that user’s MyCDX In-Box. The notification indicates that the account has been locked and the user must contact the CDX Help Desk to unlock the account. In order to re-open the account, the user must provide certain information (e.g., user’s organization, organization address, and user’s phone number) to the CDX Help Desk and successfully answer a security question that was setup during registration to verify that the individual is the CDX account holder. Upon re-establishing the user’s identity, the CDX Help Desk will reset the user’s account password to a temporary one-time-use value; the user will then receive the password to registered email address, login and create a new password~~, new security question/answer pairs and 20-5-1 question/answer set.~~  . |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **16. Procedures to revoke/reject compromised credentials** | |
|  | **Business Practices:**  When notified of a compromised password-based credential, the CDX Help Desk will immediately lock the user account associated with that credential. The user must then contact the CDX Help Desk and provide information to verify that the individual is the CDX account holder in order to reset their password and unlock their account. The user will have to provide the following information to the CDX Help Desk: user’s organization, address, and user’s phone number; as well as successfully provide the answer to the security question that was setup during registration to verify identity for account profile changes such as resetting passwords.  Also, the CSIRC determines on a case-by-case basis whether the user must reset their 20-5-1 Challenge Question/Answer pairs as well. CSIRC only requires the 20-5-1 question/answers pairs be reset in cases where the approach has been compromised. |
| **System Functions:**  See Checklist Item 13.c for a discussion on the rejection of compromised credentials by the CDX system. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **17. Confirmation of signature binding to document content** | |
|  | **Business Practices:** |
| **System Functions:**  The CDX system performs the following actions to validate the digital signature of the submitted document, created with the temporary X.509 certificate (see checklist item#5):   1. Calculation of the current message digest (hash) value of the received document using the standard SHA-1 algorithm 2. Decryption of the received digital signature using the supplied public key in order to obtain the original document hash value at signing time 3. Comparison of the current hash value with the original hash value   CDX performs this digital signature validation upon the uploading of the signed submission file to the CDX web servers. Failure to pass the digital signature validation results in a “submission failure” e-mail sent to the registered email address for the submitter. This message will be also placed into the submitting user’s MyCDX InBox. This condition (signature validation failure) is also noted in the CDX audit logs. |
| **Supporting Documentation (list attachments):**   * Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt |

|  |  |
| --- | --- |
| **Copy of Record** | |
| **18. Creation of copy of record (See 18a through 18e)** | |
| **18a. True and correct copy of document received** | |
|  | **Business Practices:**  Please see checklist item#9a for a description of the CDX COR. |
| **System Functions:**  While in transit, the integrity of the submission document is protected through the mechanisms of the HTTPS connection (see checklist item #8).  In addition, the CDX system will validate the digital signature associated with each user-signed submission document upon receipt, using the method described in checklist item #17. In cases of unsigned submission documents, CDX will immediately create a message digest of the submission document using the standard SHA algorithm and then digitally sign this message digest using CDX’s own X.509 certificate that meets minimum federal standards (currently 2048 bit key). This signed message digest, along with CDX’s public key will be packaged in the detached signature as the COR in order to provide subsequent detection of changes to the original submission content.  The CDX CROMERR Digital Signing Certificate used to sign the document demonstrates that the COR has not been altered without detection (see description of CDX Digital Signing Certificate under Checklist Item #5). Any changes to the COR are logged in transaction logs. The CDX CROMERR Digital Signing Certificate and the private key are maintained using the CDX Help Desk Tool CROMERR Administration system function. The resulting artifacts are encrypted as a single record and stored in the CROMERR database. The encryption key used to encrypt these artifacts is only known to the CROMERR Administrator. System Administrators and others with server level access cannot directly access/view/obtain the key store or its contents. The SSL Server Certificate and private key are managed separately and replaced bi-annually, providing separation of duty for audit logging between the server and the CROMERR Certificate administration. Applications which retrieve the private key must be granted system-level access and can only reference/obtain the key through the operating system-level API functions allowing the separation of duty and assurance between the application and the system logging. |
| **Supporting Documentation (list attachments):**   * Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt |
| **18b. Inclusion of electronic signatures** | |
|  | **Business Practices:** |
| **System Functions:**  CDX maintains the UserID/password as entered by the user in executing his/her e-signature in the COR. CDX also maintains an audit history of the unsuccessful UserID/password entry timestamps. Please see checklist items #5 and #9 for a description of the contents of the CDX COR and how the electronic signature is included in the COR. |
| **Supporting Documentation (list attachments):** |
| **18c. Inclusion of date and time of receipt** | |
|  | **Business Practices:** |
| **System Functions:**  Date and time of submission receipt are retained as a standard part of the CDX COR. Please see checklist item #9 for a description of the contents of the CDX COR. |
| **Supporting Documentation (list attachments):** |
| **18d. Inclusion of other information necessary to record meaning of document** | |
|  | **Business Practices:** |
| **System Functions:**  In addition to retaining the original submission file, CDX also retains submission-related metadata (such as organization ID codes, state affiliation, etc.) and other information associated with a particular submission as part of the COR. |
| **Supporting Documentation (list attachments):** |
| **18e. Ability to be viewed in human-readable format** | |
|  | **Business Practices:** |
| **System Functions:**  CDX’s ability to display the COR documents in human-readable format depends on availability of COTS product. CDX maintains COTS for XML files so that these documents can be viewed in human readable format. XSL style sheet (to apply against XML submission file(s) or metadata documents) is included if XML-style documents are included as part of, or generated during, the submission process (see checklist item #9a). Otherwise, CDX maintains the COR submission documents in human-readable PDF formats. For documents that are maintained in formats other than XML or PDF, the program office must provide the COTS product for other formats to CDX, to maintain or must maintain the COTS product itself so that the COR is available in human readable. [Program Office needs to insert process.] |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **19. Timely availability of copy of record as needed** | |
|  | **Business Practices:**  The CDX Help Desk is supplied with tools to manually retrieve and provide information concerning a copy of record (COR) within 1 business day upon request from the Program Office (PO). The requestor will need to provide the transaction ID and/or other identifying information related to the submission of interest. The submitter’s UserID and submission time period can be used when the transaction ID is unknown. |
| **System Functions:**  The COR is also available at any time following submission through the transaction history dialog. EPA program and enforcement staff who are granted access by the PO can use this dialog at any time to view and download all data content related to a submission.  The transaction history dialog provides search criteria for CORs, such as Date Range, Application Name, UserID, Transaction ID, User Affiliation Code, etc.    The CORs will be searchable and viewable for the entire length of time for which they are maintained on CDX (see question 20). |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **20. Maintenance of copy of record** | |
|  | **Business Practices:**  In order to prevent unauthorized access to the system or its data by operating personnel, CDX is operated according to the policies defined in the *CDX Separation of Duties Guide.* This document requires all CDX personnel with access privileges to the production environment to have at least a Minimum Background Investigation (MBI) clearance. In addition, the document provides for separation of duties with the goals of addressing/avoiding conflict-of-interest situations and ensuring that more than one user is involved in different stages of critical business processes, so that users are prevented from having all the necessary authority or information access to perform fraudulent activity without collusion. To achieve these goals, the document identifies the access controls, authorized actions, and minimal personnel security checks required for each defined operations role: Configuration Manager, Database Administrator, Network Administrator, Production Manager, Production Monitor, Security Manager, System Administrator, etc.  CDX adheres to the practice of providing incremental and full tape backups as part of the regular UNIX/Windows General Support System policies and procedures at the EPA's National Computer Center (NCC). Recovery of all or part of the CDX system in the event of a catastrophic failure is documented in the *CDX Contingency Plan*.  All data/information is maintained in a secured facility. All physical entry is logged and all authorized personnel have background investigations and are annually trained in security awareness, or the individuals are identified by government identifications and are escorted by individuals with personnel clearances.  Each Program Office independently specifies the retention period of the COR for their application. This information is documented in the Security Addendum produced for each CDX application. CDX will maintain the COR for a minimum of 5 years following deactivation of the associated electronic signature device unless otherwise specified by the Program Office. |
| **System Functions:**  At the completion of the creation of the COR, CDX computes a hash value of all the items that make up the COR. This hash values are signed using a CDX server private certificate. This COR signature value (and information regarding it) is saved within the database and is written to the CDX audit logs.  Other COR creation actions and related information (e.g., UserIDs, file names, document signatures, etc.) are also automatically captured by the system and written to CDX audit logs. Once per day the CDX system copies the contents of these logs to a separate server stored in XML format and applies a separate digital signature using CDX’s digital signing certificate to prevent/identify tampering with log file content. CDX then performs digital signature validation on the newly signed record of the daily CROMERR submissions. This process provides an additional independent means of validating the integrity of COR content and submission history apart from the audit log database server. This ensures that the submissions were not tampered with. In the event that COR integrity is compromised an email is sent to the CROMERR Administrator containing affected document identifiers.  All information related to the COR is stored/retained in Oracle databases. These Oracle databases are maintained on servers providing storage via a redundant array of independent disks (RAID). These RAID systems detect and address any hardware-related storage errors. To address DBMS vendor-related errors, CDX employs automated database backup procedures that make use of the Oracle Recovery Manager product, allowing for rollback/recovery of database objects at nearly any point in time. CDX also makes use of standard database vendor audit tracking functions for all COR database tables, thereby recording any access to (or modification of) this information by an authorized or unauthorized user.  All CDX system files (including the databases) are automatically backed up on magnetic tape, either on a daily (incremental) or weekly (full) schedule, for permanent off-site storage.  CDX maintains CORs as a combination of binary large object (BLOB) files and non-BLOB objects. The BLOB files consist of the submission files that were signed and certified to by the user (assuming that signature was required). Non-BLOB objects include such metadata as the encrypted message digest, timestamps, transaction IDs, and stylesheets to allow display of the BLOB files in human readable formats. To preserve/recover storage space and remove obsolete data, CDX contains an automated “clean-up tool” that monitors the COR record archive on a daily basis and removes submission-related BLOB files that have passed their expiration period (based on submission date/time stamp); non-BLOB objects, however, are retained for historical reference. This action is recorded in the CDX audit log files and includes the date/time stamp of the removal action. This tool is configurable to follow the retention period guidelines specific by each Program Office for their application. BLOB files remain accessible for recovery, as necessary, through historical backup tapes. |
| **Supporting Documentation (list attachments):**   * Attachment 9 – CDX Separation of Duties Guide * Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt |