

<b>CROMERR System Checklist</b>	
<b>Item</b>	<p>Attachment 1 – EPA CDX Help Desk Digital Cert Mgmt Procedures.pdf</p> <p>Attachment 2 – CDX Registration Maintenance Rules of Behavior Release 1.0.doc</p> <p>Attachment 3 – RegMain Procedures 12-7-2005.pdf</p> <p>Attachment 4 – Digital Signature Trust Local Registration Authority Handbook.pdf</p> <p>Attachment 5 – Sample CDX Digital Signature Agreement (DSA).pdf</p> <p>Attachment 6A - Process flow for 20-5-1_ e-signature(temporary) certificate binding.ppt</p> <p>Attachment 6B - Process flow for Hybrid(20-5-1)_ PKI certificate binding.ppt</p> <p>Attachment 7 – Sample of Review and Confirmation dialogs.doc</p> <p>Attachment 8 – Sample of Certification and Confirmation Page for eIUR.doc</p> <p>Attachment 9 – CDX Separation of Duties Guide</p> <p>Attachment 10 - CDX Contingency Plan 04-28-06.doc (Available upon request)</p> <p>Attachment 11 - 20-5-1 Questions.doc</p> <p>Attachment 12 - 20-5-1 e-Signature Registration Process V1.ppt</p> <p>Attachment 13 - PKI Certificate Registration Process V1.ppt</p> <p>Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt</p> <p>Attachment 15 – Content of X.509 Certificate.ppt</p>

<b>Registration (e-signature cases only)</b>	
<b>1. Identity-proofing of registrant</b>	
	<p><b>Business Practices:</b></p> <p>During the user registration process CDX provides the user with an Electronic Signature Agreement (ESA) that must always be completed, signed (handwritten) by the user and the company's authorizing official, and mailed to the CDX Help Desk prior to account or role activation (the latter only if the account was previously established for other purposes). This is done for both PKI applications and non-PKI applications that use e-signature functions. Per CROMERR 3.2000(b)(5)(vii)(C), the receipt of a signed ESA will be sufficient proof of the user's identity.</p> <p>See question 4 for further discussion of the ESA and a sample/attachment of the CDX Digital</p>

### Signature Agreement (DSA) agreement.

Through the use of the ESA, CDX asks that the company's authorizing official perform (or acknowledge that their company has performed) the duties noted in NIST 800-63 for assuring that the applicant is in possession of a valid Government ID. By providing their handwritten signature on the ESA, the company's authorizing official acknowledges:

- (1) That they have validated that the prospective user is in possession of a valid current primary Government Picture ID that contains the applicant's picture, and either address of record or nationality (e.g. drivers license or passport)
- (2) That they have inspected said ID to compare picture to applicant, have recorded the ID number and issuer of the ID as well as the address and Date of Birth, as so indicated on the Government Picture ID.
- (3) That they will keep a record of the above information for a minimum of five years after user employment termination or change in position

Upon receipt of the signed ESA, the CDX Help Desk validates the information on the ESA with the information provided by the user on the ESA and during the registration process by making telephone contact with the user's authorizing official/employer to confirm business employment and submitter authorization per the standard CDX Help Desk user identify proofing procedure. An example of this procedure is contained in the *CDX Help Desk Digital Certificate (PKI) Management Procedures* document (see Attachment 1).

In addition to the above, if this is a PKI flow the user's information is also validated by the CDX Help Desk at/with the CDX-approved certificate authority (CA). The CDX Help Desk then updates the ESA with the CA-provided certificate serial# issued to this specific CDX user account.

The CDX Help Desk stores the received ESA in a paper-based filing system. The CDX Help Desk currently retains the ESAs for all signing credentials issued on behalf of CDX for a minimum of five years after account deactivation and/or certificate revocation.

If the Program office performs this identify-proofing function, then they would perform these duties in a manner similar to the above.

**System Functions:**

For user-initiated registration requests, the CDX system presents each user with a web-based link to download or print the Electronic Signature Agreement (ESA) during the registration process. Before the user can exit this screen, they are presented with instructions on how to complete the ESA and told of the follow-on actions to be taken upon receipt of the ESA 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.

For Program Office (PO)-initiated registration requests, the CDX system pre-populates the CDX system's registration tables with the user information provided by the PO. The CDX system then generates a unique, one-time-only Customer Retrieval Key (CRK) for each prospective user account. The CRK is a Soundex-like version of the supplied user name concatenated with a 5 digit random number. A Soundex-like algorithm is used in this process in order to differentiate between users who might otherwise have provided similar information. CDX uses the first letter of each individual word found followed by 3 Soundex digits. For example:

	Soundex	Random#	
John Public =	J100P435	+ 23582	= CRK Value = J100P43523582
John Q. Public =	J100Q10P435	+ 24562	= CRK Value = J100Q10P43524562

The CDX Help Desk provides these CRKs to the PO who then distributes them in a controlled fashion to each sponsored user. The distribution mechanism varies by Program based upon user community size, but distribution by mail to the user's registered mailing address is the most common practice.

Each sponsored user then inputs a special CDX URL and the CRK into their web browser and is forwarded automatically to their pre-populated CDX registration web pages where they complete their registration and obtain/submit their ESA to the PO or CDX Help Desk as stated in the previous paragraph.

**Supporting Documentation (list attachments):**

Attachment 1 - EPA CDX Help Desk Digital Cert Mgmt Procedures.pdf

<b>1a. (priority reports only) Identity-proofing <i>before</i> accepting e-signatures</b>	
	<p><b>Business Practices:</b></p> <p>N/A</p>
	<p><b>System Functions:</b></p> <p>N/A</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<b>1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)</b>	
<b>1bi. (priority reports only) Verification by attestation of disinterested individuals</b>	
	<p><b>Business Practices:</b></p> <p>N/A</p>
	<p><b>System Functions:</b></p> <p>N/A</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<b>1bii. (priority reports only) Information or objects of independent origin</b>	

	<b>Business Practices:</b> N/A
	<b>System Functions:</b> N/A
	<b>Supporting Documentation (list attachments):</b>

**1b-alt. (priority reports only) Subscriber agreement alternative**

	<b>Business Practices:</b> N/A
	<b>System Functions:</b> N/A
	<b>Supporting Documentation (list attachments):</b>

**2. Determination of registrant's signing authority**

	<b>Business Practices:</b>
	<p>Program Offices are responsible for establishing, documenting, and following the pre-set policy and procedures defined by their program to validate a prospective user's registration information and the organization that they represent, in order to ensure the accuracy of this information and the appropriateness of the requestor to be granted signatory authority for their organization.</p> <p>CDX assists each Program Office in carrying out these actions by identifying the appropriate CDX</p>

user registration and authorization programmatic functions that can be used to support the Program Office's signatory approval process – such as including links to the appropriate forms, etc.

In addition to, or as part of the ESA (see question#4), evidence of submission authority as collected by CDX as part of the registration process is a request for a Sponsor Letter from the user's sponsoring organization. This letter must be on company letterhead and include a signed attestation by an official at the company (at the level defined by the Program Office), that the individual registering works for the company and is authorized to submit on its behalf. The Sponsor Letter is then mailed to the Program Office by the prospective user. The PO (or the CDX Help Desk on their behalf) stores the Sponsor Letter in a paper-based filing system. The PO (or the CDX Help Desk) shall retain the sponsor letter for a period of 5 years after being notified of the signatory's departure from their sponsoring organization by a company official.

The CDX Help Desk may be designated by the Program Office to perform signatory authority verification/approval actions on their behalf when so requested and trained in the appropriate procedures by the Program Office.

CDX employs a role-based user access authorization system. The registrant's role-based access to CDX applications will not be activated until the identity-proofing requirements are completed and access authorization is granted by the Program Office or by the CDX Help Desk in accordance with each Program Office's approved role authorization approval process.

Each Program Office Point of Contact (POC) that is allowed to serve as a delegated CDX user registration authority 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. These POCs are known as registration maintenance users (RMAMs). 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).

Along with other obligations, the *CDX Registration Maintenance Rules of Behavior* document specifies that each POC/RMAM shall maintain a record of those individuals whose identity has been verified, and the steps taken to verify his/her user identity.

These records shall be maintained by the POC to provide evidence of identity proofing to relying

parties as necessary. The specific identity proofing and registration process for a program office application shall be performed according to a documented program office written policy or practice statement.

The CDX Help Desk shall require each POC/RMAM mail a copy of the CDX "Rules of Behavior" acknowledgement statement to the CDX Help Desk within thirty days of their sponsorship. Any POC/RMAM whose acknowledgement statement is not received in this period will have his/her access revoked by the CDX Help Desk.

The CDX Help Desk stores the RMAM's *CDX Registration Maintenance Rules of Behavior* acknowledgement in a paper-based filing system. The CDX Help Desk currently retains the CDX "Rules of Behavior" acknowledgement for a minimum of five years after RMAM account/role deactivation.

#### **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 organizational authority to the Program Office or CDX Help Desk (as delegated). This is done 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.

The CDX system provides a web-based mechanism (called Registration Maintenance) for approved Program Office representatives (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 both the use of User ID/password credentials and digital certificates.

#### **Supporting Documentation (list attachments):**

Attachment 2 – CDX Registration Maintenance Rules of Behavior Release 1.0.doc Attachment 3 – RegMain Procedures 12-7-2005.pdf
--

### 3. Issuance (or registration) of a signing credential in a way that protects it from compromise

#### **Business Practices:**

CDX supports two kinds of signing credentials; e-signature credentials that are authorized for creation/use through the real-time input and validation of a user's system identity credentials plus some other user-provided secret(s), i.e., a pin/password-based approach, and industry standard PKI digital certificates.

Issuance and selection of a CDX User Id and Password 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
- Will 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.

CDX's PKI-related flows use a third party Certificate Authority (CA) to provide the business class digital certificates used as signing credentials. The X.509 digital certificates issued by the CDX CA contain the following information:

- Name and Contact information of the CA;
- Name of the subscriber/certificate holder;
- Public Key of the Subscriber;
- Public Key of the CA;

- Signature hash provided by the CA (Used to validate issuance by the appropriate CA);
- Unique certificate serial number;
- The certificate's operational period (i.e., expiration date).

**System Functions:**

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.

CDX e-Signature Enabled and PKI Enabled Applications: CDX uses a combination of the account holder's CDX User ID, CDX Password and a randomly selected user-specified secret in order to apply an e-signature or PKI signature to submission documents.

Use of a randomly selected user-specified secret is known as the 20-5-1 security question/answer technique.

The user specifies their selection of a CDX User ID and Password as part of the general CDX user registration process. This CDX User ID is automatically captured on/provided with the ESA submitted by the user. The User ID and password must each be at least 8 characters long and contain a mixture of letters and numbers. 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:

- User ID and password are concatenated together (separated by a pipe ( | ) character)
- The concatenated value is hashed using the SHA-1 algorithm
- The resulting hash is hashed again using the SHA-1 algorithm
- The Hex value of the resulting *double* hash is saved to the database with a date/time stamp

*Please see attachment 14 for a depiction of all the various hashing processes employed by CDX.*

CDX retains all previously entered passwords for this user in order to prevent password re-use. Passwords are automatically expired by the CDX system every 90 days per standard EPA policy. Users are sent an out-of-band email notifying them of this occurrence along with instructions on how to reset their password.

Subsequent authentication of this user upon login through the use of this password is done through comparison of the double hash value of the current user-entered password with the double hash value from the most recent password establishment. Other user identifying information is also collected during the user registration process such as; Name Title, First Name, Middle Initial, Last Name, Name Suffix, Email Address, Street Address, City, State, Zip Code, and Daytime Phone Number.

As the user may have a need to alter some aspect of their account profile in the future, the system requires that the user also specify a secret question and secret answer in order to successfully respond to a CDX Help Desk or Self-Service identity challenge. Knowledge of both the question and answer would help confirm that this user is the establisher of the original account (along with use/validation of other identity information). The secret portion of this information is secured as per the account password, but is not otherwise used in the 20-5-1 e-Signature process.

If the user has selected registration in an e-Signature or PKI enabled application, CDX requests acceptance of the ESA completion instructions as well as other terms and conditions. Upon user acceptance, 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 double-hash of the user's ID and password
- The system concatenates the user ID, question #, user-supplied answer, and latest double-hash of the user's ID and password
- The concatenated value is SHA-1 hashed
- The resulting hash is hashed again using SHA-1
- The Hex value of the resulting *double* hash is saved to the database with a date/time stamp

Use of the CDX User ID in the hash computation ensures that these answers are tied to a particular CDX account.

The user may need to update their user profile in CDX at a later date in order to reset their account password or reselect/re-enter 20-5-1 questions/answers. The user must supply the secret question/answer during the registration process to perform this action in a self-service manner. All updates to this information are secured as stated above and the user is sent an out-of-band email message notifying them of an account modification action. Note that the registered email address of the user can never be changed – thus the original owner of that registered email address will always continue to receive such notifications, even in the event that the account is compromised.

Receipt and validation of the Electronic Signature Agreement is required before activation of the user's signatory role as discussed in question 4.

Further use of User ID/Password information or the 20-5-1 secret(s) in the e-signature process are described in question 5.

CDX PKI Enabled Applications Only: Selection/securing of CDX User ID, Password, and 20-5-1 secrets for users selecting registration for an application requiring PKI certificates is performed in accordance with the methods described above. After acceptance of the ESA terms and conditions, the user is re-directed by the CDX web servers to a special CDX-only HTTPS URL on the authorized CA system where they are prompted to enter identity information and create a pass phrase (Case sensitive 8-30 characters, letters, numbers, and some special characters allowed). The CA follows industry business practices for securely collecting this user identity information and upon completion marks the certificate issuance as "pending issue".

Upon receipt and validation of the ESA information, the CDX Help Desk uses a special smart card-enabled Local Registration Authority (LRA) credential and a web browser to access another special CDX-only HTTPS URL on the CA site. The CDX Help Desk then obtains the one-time-only-use activation code and the certificate serial number from the CA and marks the credential as "approved for issue". The activation code and a special secure retrieval URL for the CA site is then transferred to the user by the CDX Help Desk by making contact with that user using their supplied registration contact information – including the user's registered email address. This process is documented in the *Digital Signature Trust (an IdenTrust Company) Local Registration Authority Handbook* (see attachment 4).

The user accesses the secure URL with their one-time-use activation code and the special pass phrase that they created upon first visiting the CA site. Upon validation of this information, the CA then downloads the CA-signed certificate and its associated private key to the user's local key/certificate store. This key/certificate store is password protected on the workstation as per the mechanisms of the workstation OS provider.

Note: The CDX CA provider is a member of the GSA ACES program. As such, key pair generation by the CA is performed using only approved cryptographic standards, published by the National Institute of Standards and Technology in Federal Information Processing Standards Publication, FIPS PUB No. 140-1, "Security Requirements for Cryptographic Modules" (FIPS 140-1). Each CA-issued certificate is digitally signed by the CA provider to ensure that its information has not been altered or duplicated and affords CDX the opportunity to validate the CDX CA as the authorized issuer.

Further use of the digital signature credential in the signature process is described in question 5.

Additional Note: 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.

**Supporting Documentation (list attachments):**

Attachment 4 – Digital Signature Trust Local Registration Authority Handbook.pdf

Attachment 11- 20-5-1 Questions.doc

Attachment 12 - 20-5-1 e-Signature Registration Process V1.ppt

Attachment 13 - PKI Certificate Registration Process V1.ppt

Attachment 14 – CDX Hashing Diagrams 08-31-2007.ppt

#### 4. Electronic Signature Agreement

**Business Practices:**

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 ESA is always used for identity proofing purposes and may optionally be used for collecting sponsorship (i.e., authorization-related) information (at the discretion of the Program Office). In cases where the two purposes are separated, CDX uses a sponsor letter in addition to the ESA (see question #2).

In the ESA, users must minimally provide the following information: Company Name, Address/City/State/Zip, Site Name, Signatory Name, Email Address, Wet Ink Signature, Date, and Title. CDX also requires that the user include their selected CDX User ID on the form. The CDX Help Desk will not approve an ESA that does not contain all of the above information, as this signed document is used to link the uniquely named/identified individual to their CDX-issued authentication credentials.

The Program Office may also request that additional terms be included in the ESA.

Each registrant must provide a handwritten signature on this ESA and mail it, along with other documents specified by the program offices - such as an official signatory authorization letter on Company Letter Head, to the CDX Help Desk or the sponsoring Program Office. By affixing their signature users explicitly provide their agreement to adhere to the CDX policies, terms, and conditions listed in the agreement.

Minimally the ESA terms impart that the user imparted signatory authority:

- (1) Agrees to protect the signature from use by anyone except themselves, and to confirm system security with third parties where necessary. Specifically, they agree to maintain the secrecy of the code where the signature is based on a secret code;
- (2) Understands and agrees that they will be held as legally bound, obligated, or responsible by

	<p>the use of their electronic signature as they would be using a hand-written signature, and that legal action can be taken against them based on their use of the electronic signature in submitting an electronic document to the US EPA's CDX;</p> <p>(3) Agrees never to delegate the use of their electronic signature or make their signature available for use by anyone else;</p> <p>(4) Understands that whenever they electronically sign and submit an electronic document to the US EPA's CDX, acknowledgments and a copy of my submissions will be made available to them;</p> <p>(5) Agrees to review the acknowledgments and copies of documents they electronically sign and submit to the US EPA's CDX;</p> <p>(6) Agrees to report to the US EPA, within twenty-four hours of discovery, any evidence of the loss, theft, or other compromise of any component of their electronic signature;</p> <p>(7) Agrees to report to the US EPA, within twenty-four hours of discovery, any evidence of discrepancy between an electronic document they have signed and submitted and what the US EPA's CDX has received from them.</p>
	<p><b>System Functions:</b></p> <p>The CDX web-based registration system provides the user the opportunity to obtain and print the ESA either during the new user registration process or during existing user account profile maintenance. Subsequent processing of the ESA is handled by a business practice.</p> <p>The system will pre-populate user information on the ESA obtained in the registration process, specifically including the user's selected CDX user account ID. The CDX Help Desk will not approve an ESA that does not contain a valid CDX user account name.</p> <p>When an ESA has been accepted and validated by the CDX Help Desk or by the PO application's delegated registration maintenance administrator (RMAM), they use the Registration Maintenance tool to grant access to the application. The CDX system logs this action and automatically sends the prospective user an email (to their CDX registered email address) upon this event, as well as to all RMAMs in the same approving group for that PO.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

	Attachment 5 - Sample CDX Digital Signature Agreement (DSA).pdf
--	---

<b>5. Binding of signatures to document content</b>	
	<p><b>Business Practices:</b></p> <p>CDX supports two signing methods, use of CDX account information and user-proprietary secrets to authorize the creation/use of an e-signature signing credential (known as the 20-5-1 method) and application of a standard X.509 PKI digital certificate (known as the PKI method).</p> <p>Creation of the e-signature signing credential is done at document submission time; creation of the standard X.509 digital certificate is done some time prior to submission and is handled by the CDX-approved CA (see question 3).</p>
	<p><b>System Functions:</b></p> <p><u>CDX e-Signature and PKI Enabled Applications:</u> During the submission process, users are informed of the implications of their review/certification/signing of submission documents as per the mechanisms described in questions 6 and 7. After their acknowledgement of these conditions, CDX downloads vendor-supplied client side controls to the user’s workstation and prompts the user for their current account password. This password, along with the current known User ID from the CDX session management table is then hashed as per the procedure noted in question 3 and compared to the current User ID/Password combination. If this combination is valid, it is immediately used to authorize access to a randomly selected question/answer pair from the list of five selected 20-5-1 questions. This re-establishment of the password ensures that the user has not walked away from their workstation while the submission action is in progress, thereby allowing others to select submission files or perform other actions while the account owner is not present.</p> <p>When a valid User ID/Password combination is provided, the system will randomly select one of the five questions selected by the user during the 20-5-1 registration process for the application and request that the user provide the correct response to that question. The current user-supplied answer is then hashed as per the procedure noted in question 3 and then compared with the answer as originally recorded. The user is provided with three attempts to recall and enter this single 20-5-</p>

1 question/answer combination correctly. A third failed attempt results in abandonment of the submission/signing procedure as well as a user account lock-out and indicators in the CDX audit trail and an automated out-of-band user e-mail that the account has been disabled due to validation failure.

Completion of the signature process is performed using either a temporary private key generated on the client workstation or a the private key associated with a CA-provided PKI certificate as described below:

CDX e-Signature Enabled Applications Only: If the user-supplied answer to the 20-5-1 challenge is correct, CDX uses vendor-supplied client side controls (currently ASPEncrypt) to create a 1024-bit public/private key pair using the properly hashed User ID/Password. The public key from this process is stored in a temporary X.509 signing certificate on the user workstation that also includes current user/session information. This temporary X.509 certificate is signed by a CDX server process call using a CDX server private certificate. See attachment 15 for the content of this temporary X.509 certificate.

A message digest for the submission document (or documents if multiple documents make up the submission) is created on the client by vendor-supplied client side controls using the SHA-1 algorithm and then this message digest is encrypted using the user's private key (again using the SHA-1 algorithm). The temporary X.509 certificate, the submission document, and the document signature (encrypted document message digest) are then uploaded to the CDX server and stored in a COR record with a unique transaction ID.

CDX PKI Enabled Applications Only: If the user-supplied answer to the 20-5-1 challenge is correct, the user is provided with three attempts to recall/enter the correct pass phrase for their private key. A third failed attempt results in abandonment of the signature/submission process along with a CDX audit trail entry and an automated out-of-band user e-mail that a failed signing action has been attempted.

If the user-supplied pass phrase for their private key is successful, a message digest for the submission document is created on the client by vendor-supplied client side controls using the SHA-1 algorithm and then this message digest is encrypted using the user's private key (again using the SHA-1 algorithm). The X.509 digital certificate, the

	<p>submission document, and the document signature (encrypted document message digest) are then uploaded to the CDX server and stored in a COR record with a unique transaction ID.</p>
	<p><b>Supporting Documentation (list attachments):</b></p> <p>Attachment 6A - Process flow for 20-5-1_ e-signature(temporary) certificate binding.ppt                  Attachment 6B - Process flow for Hybrid(20-5-1)_ PKI certificate binding.ppt Attachment 15 - Content of X.509 Certificate.ppt</p>

<p><b>6. Opportunity to review document content</b></p>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>Upon completion of data/metadata entry and/or submission file selection by the user, the CDX system will display a "review and confirm" dialog consisting of one or more pages of read-only information regarding the potential submission. This dialog allows the user the opportunity to review all of their information prior to final submission. 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 previous set of data/metadata collection web forms.</p> <p>See the attachment for an example of these two types of dialogs.</p> <p>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 abandon their potential submission.</p>

	<p>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.</p>
	<p><b>Supporting Documentation (list attachments):</b></p> <p>Attachment 7 – Sample of Review and Confirmation dialogs.doc</p>

**7. Opportunity to review certification statements and warnings**

	<p><b>Business Practices:</b></p> <p>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.</p>
	<p><b>System Functions:</b></p> <p>Prior to digitally signing or accepting a signed submission document from the user, 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 digital 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.</p> <p>Note: Some submission files may be signed outside the scope of the CDX system prior to their use in a CDX submission scenario. In this case, CDX does not re-sign the document; however, the system does make the user acknowledge a signature certification statement during the submission process, as it cannot be assured that the user was apprised of the implications of affixing their electronic signature to the submission document by their offline signing application.</p> <p>An example of an application certification statement displayed by the CDX system reads: "I certify under penalty of law that I have personally examined and am familiar with the information I</p>

	<p>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. ”</p> <p>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.</p>
	<p><b>Supporting Documentation (list attachments):</b> Attachment 8 – Sample of Certification and Confirmation Page for eIUR.doc</p>

<b>8. Transmission error checking and documentation</b>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>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.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<b>9. Opportunity to review copy of record</b>	
<b>9a. Notification that copy of record is available</b>	

**Business Practices:**

The Copy of Record (COR) for CDX consists of:

1. The submission file (or files) – along with their associated signatures and signatory public keys as appropriate
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 its associated signature and signatory public keys as appropriate
3. A unique Transaction ID associated with the submission
4. The date/time stamp of submission
5. Certificates associated with this submission (needed to tie the public key to a particular user)

An XSL style sheet (to apply against XML submission file(s) or metadata documents) may be included if XML-style documents are included as part of, or generated during, the submission process.

For submission files not signed by the submitter, CDX will sign the file using its own private 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.

For encrypted submission files, the submitting user's public key is also included as part of the COR. This allows a backend system to use this key on their own system to encrypt subsequent communications and other submission related documentation for post -submission consumption by the submitter. This allows CDX to make a submitter-readable Copy of Record available in cases when the encrypted original would ordinarily only be readable by the Program Office system that supplied the original encrypting key.

Users are notified of the availability of their CDX Copy of Record through 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 user ID, date/time of submission, transaction ID, and the file name(s) of each submission file are generally included in this message by default.

	<p><b>System Functions:</b></p> <p>CDX provides each registered user with browser-based access to an individualized messaging In-box function (called MyCDX In-box).</p> <p>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 out-of-band email notification to a user’s registered email address where appropriate.</p> <p>The MyCDX In-box and out-of-band email messages contain information concerning the success/failure or the data submission process as well as other instructions and URL links relevant to the submitted information. Such instructions indicate how to access/browse/download their Copy Of Record (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 user ID, date/time of submission, transaction ID, and the file name of the original submission.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<p><b>9b. Creation of copy of record in a human-readable format</b></p>	
	<p><b>Business Practices:</b></p> <p>CDX receives submission files in multiple native formats. These include text (.TXT), Extensible Markup Language (XML), Portable Document Format (.PDF), Comma-Separated Values (.CSV), Zip data compression format (.ZIP), and Microsoft Word (.DOC).</p>
	<p><b>System Functions:</b></p> <p>The copy of record 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</p>

	<p>tables, which reside on an Oracle database server. Uploaded submission files and any necessary related XSL files are stored in the archive database as BLOB types due to their variable size – and thus retain their native form. 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.</p> <p>In cases where the user-supplied submission input is 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. It is this PDF that becomes the COR submission document. This procedure is used even for those web forms that ordinarily write their data directly to database tables.</p> <p>In cases where the original submission file is received from the user in an encrypted form that is originally only consumable by the back end Program Office system, the receipt of a such suitably re-encrypted files from the Program Office system will be made available by CDX to the user at a later time.</p> <p>See answer 9C for information regarding user consumption of COR-related items.</p> <p><b>Supporting Documentation (list attachments):</b></p>
<p><b>9c. Providing the copy of record</b></p>	
	<p><b>Business Practices:</b></p> <p><b>System Functions:</b></p> <p>Two mechanisms are provided to allow the system user to access/download their copy of record on CDX – a MyCDX In-box message URL link and a transaction history dialog. Both options are available for every submission, however, the user is likely to use the transaction history to look for and retrieve older submissions, based on its search capabilities.</p> <ul style="list-style-type: none"> <li>• Inbox Option: The users MyCDX In-box provides the user with a list of messages pertaining to their submissions. Those messages related to submissions and submission processing contains</li> </ul>

	<p>links to the Copy of Record along with instructions on how to download and view any copy of record information.</p> <ul style="list-style-type: none"><li>• Transaction History Option: In addition to responding directly to an email notification concerning the COR, a submitter can also log into CDX and 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.<ul style="list-style-type: none"><li>○ If the COR is the original submission document, the document is available as soon as the submitter completes the submission the data.</li><li>○ If part of the COR needs to be "processed and supplied" by a backend application, the backend 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.</li><li>○ If any portion of the COR is encrypted for transmission to the back-end, CDX relies on the back-end to re-encrypt the COR with the user's public key and submit that portion of the COR back to CDX for consumption by the user. CDX will relate that COR data item back to the original submission through the transaction ID.</li></ul></li></ul>
	<p><b>Supporting Documentation (list attachments):</b></p>

**10. Procedures to address submitter/signatory repudiation of a copy of record****Business Practices:**

The anticipated reasons a user would want to repudiate a COR include:

1. The user claims they did not submit the COR.
2. The user claims that their signing credential was used inappropriately.
3. Erroneous data was submitted.

If the user disputes their submission of the COR, the Program Office can then contact the CDX Help Desk to obtain the submission data and associated metadata, the date/time of submission, the submitting User ID, the user audit trail log, the public key, and the signature hash that were stored with the submission (the last two items as applicable). That information, along with items from any ESA/Sponsor Letters would be used to establish the identity and authority of the submitter with respect to a particular submission. Receipt of a request for assistance from the Program Office would be captured in the CDX Help Desk ticketing system.

If it is found that the user did not submit the COR, the user's signature credential has been compromised. The Program Office is required to contact the CDX Help Desk and lock the user's account to prevent additional compromises. The extent of the compromise will be assessed to determine whether any additional submissions need to be repudiated. The user and the Program Office will also investigate how the account may have become compromised in order to prevent future occurrences.

The CDX system provides for submission of revisions to submitted documents in the same manner as the original submission. The individual Program Offices sponsoring CDX applications are responsible for establishing, documenting, and following the policy and procedures defined by their program to accurately process the replacement/supplemental submission. Internally, CDX treats these re-submissions as a distinct new COR.

**System Functions:**

For CROMERR-related applications, the system will provide users with access to their individualized submission history function. This function allows the user to browse/search for any potentially suspect submissions and initiate repudiation-related communications with Program Office

	<p>representatives.</p> <p>The CDX system provides a web-based mechanism for the CDX Help Desk to lock a user's account, revoke a digital certificate, or re-issue signing credentials.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<b>11. Procedures to flag accidental submissions</b>	
	<p><b>Business Practices:</b></p> <p>If a user accidentally submits the wrong file or submits faulty data, they will notify the appropriate EPA Program Office Point of Contact (POC) and likely be asked to resubmit. Actions taken by the backend system in this event are Program Office specific, but would nominally include formal notification of an error being reported via mail or email and invocation of data removal/rejection procedures.</p>
	<p><b>System Functions:</b></p> <p>The CDX system allows resubmission of data if the user finds an error in the original submission and per the Program Office's regulations regarding corrections and/or re-submittals.</p> <p>CDX provides multiple system mechanisms to prevent and identify accidental or erroneous submissions.</p> <ol style="list-style-type: none"> <li>1. During data entry or file selection:                     <ol style="list-style-type: none"> <li>a. 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.</li> <li>b. By validating the necessary inclusion of all dependent data fields.</li> <li>c. By providing users with the opportunity to interactively browse to select the submission file, they intend to submit instead of being asked to type in the file name and path.</li> <li>d. By performing simple file validation checks on user-entered or selected file names, such</li> </ol> </li> </ol>

	<p>as properly constructed/formatted file names and inclusion of expected file extensions.</p> <ul style="list-style-type: none"> <li>e. By automatically providing help to the user in finding the signed versions of their submission file(s) on their file system where necessary.</li> </ul> <p>2. During the submission process:</p> <ul style="list-style-type: none"> <li>a. Users are given the opportunity to review the dynamic field metadata entries related to submission in a read-only manner prior to being able to submit.</li> <li>b. Users must confirm all submission actions via a confirm/certify page.</li> </ul> <p>3. Upon/after submission:</p> <ul style="list-style-type: none"> <li>a. 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.</li> <li>b. 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</li> <li>c. Submission files are subject to validation of proper file types (XML vs .ZIP), etc. and users are notified by email if errors are found.</li> <li>d. Submitters receive an email confirmation and in-box notification of every submission, even those that are rejected due to processing errors.</li> <li>e. 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.</li> <li>f. Users can review the CORs of all previous submissions by accessing their MyCDX In-box or submission history function.</li> </ul>
	<p><b>Supporting Documentation (list attachments):</b></p>

<p><b>12. (e-signature cases only) Automatic acknowledgment of submission</b></p>	
	<p><b>Business Practices:</b></p>

	<p><b>System Functions:</b></p> <p>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.</p> <p>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 identifying the User ID 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. 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.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<b>CROMERR System Checklist</b>	
<b>Signature Validation (e-signature cases only)</b>	
<b>13. Credential validation (See 13a through 13c)</b>	
<b>13a. Determination that credential is authentic</b>	
	<p><b>Business Practices:</b></p>

	<p><b>System Functions:</b></p> <p>See the answer to question#3 for how CDX securely issues and protects the Pin/Password and/or PKI credentials.</p> <p>See the answer to question#5 for how CDX creates the temporary X.509 certificate for Pin/Password Enabled Flows.</p> <p>The CDX system determines the authenticity of the signing credential(s) attached to submission documents as follows:</p> <p>CDX e-Signature Enabled Applications: For the 20-5-1 security question/answer data flows, CDX validates that the certificate issuer signature contained in the temporary submission-signing x.509 certificate matches the official CDX signing certificate. If the issuer information is incorrect, then the submission is rejected and an out-of-band e-mail will be sent to the registered email address for the submitter and a message will be placed into the submitting user's MyCDX in-box. This condition is also noted in the CDX audit logs.</p> <p>CDX PKI Enabled Applications: CDX validates that the X.509 certificate used was issued by the CDX-approved CA and that the certificate is not expired. If the issuer information is incorrect, then the submission is rejected and an out-of-band e-mail will be sent to the registered email address for the submitter and a message will be placed into the submitting user's MyCDX in-box. This condition is also noted in the CDX audit logs.</p> <p><b>Supporting Documentation (list attachments):</b></p>
--	---

<b>13b. Determination of credential ownership</b>	
	<b>Business Practices:</b>

	<p><b>System Functions:</b></p> <p>CDX e-Signature Enabled Applications: For the 20-5-1 security question/answer data flows, CDX validates that the UserID/Password hash information contained within the user identity portion of the temporary x.509 certificate matches the submitter’s CDX UserID/Password hash as stored in the system’s Identity Management tables. 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.</p> <p>CDX PKI Enabled Applications: CDX compares the certificate serial number used to sign the document with a CDX Oracle table that contains the mapping of CDX User IDs with their associated certificate serial numbers. If the serial number does not match the known serial number assigned to the submitting user’s User ID, then the submission is rejected and an out-of-band e-mail will be sent to the registered UserID for that certificate serial number and a message will be placed into that user’s MyCDX in-box. This condition is also noted in the CDX audit logs.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<b>13c. Determination that credential is not compromised</b>	
	<p><b>Business Practices:</b></p> <p>None</p>
	<p><b>System Functions:</b></p> <p>CDX e-Signature Enabled Applications: For the 20-5-1 security question/answer data flows, the signing instrument is a one-time-use-only X.509 certificate. This temporary certificate is only</p>

	<p>generated after prompting the user for their account Pin/Password and the Secret Answer to one of their five selected security questions. The hashed values of the current user-supplied Pin/Password and the Secret Answer are then compared to the original hash values stored in the user registration database. If the values do not match, the user is not allowed to generate the temporary X.509 certificate and the failed signing attempt is logged in the CDX audit log tables. See the answer to question #3 for specifics regarding User Pin/Password and Secret Answer protection.</p> <p>CDX PKI Enabled Applications: For the PKI enabled data flows, the signing instrument is a standard X.509 digital certificate provided by the CDX-approved CA. To ensure additional protection in the event a user's X.509 certificate passphrase get compromised, users will initially be challenged with providing a correct response to their 20-5-1 security question/answer. If the user-supplied answer to the 20-5-1 challenge is correct, the user is prompted to provide the secret pass phrase protecting the private key that correlates with their CA-supplied X509 certificate. Entry of three invalid pass phrases prohibits completion of the document signing process. Upon receipt of a PKI-certificate signed document, CDX will complete the certificate validation process by checking the certificate's current revocation status using the CDX hosted GSA ACES Certificate Arbitration Module (CAM). The CDX CAM server will contact a CDX-approved CA to validate the certificate serial number against the CA's Certificate Revocation List (CRL) via an Online Certificate Status Protocol (OCSP) connection. The CA will provide a certificate status indicator (valid, revoked, expired, suspended, cert unknown) response back to the CDX CAM. If the response is anything other than "valid", then the submission is rejected and an out-of-band e-mail will be sent to the registered email address of the UserID making the submission and a message will be placed into that user's MyCDX in-box. This condition is also noted in the CDX CAM audit log.</p> <p><b>Supporting Documentation (list attachments):</b></p>
--	--

<b>14. Signatory authorization</b>	
	<p><b>Business Practices:</b></p> <p>Each application Program Office is responsible for identifying the specific requirements to be used for</p>

	<p>the determination of a registrant’s signing authority. See question #2 for additional information.</p>
	<p><b>System Functions:</b></p> <p>CDX makes use of role-based user access controls. Only those users who have been granted approval to make use of a signatory role for their application by the CDX Help Desk or the Program Office RMAM are allowed access to the web-based dialogs and web services needed to perform signing actions. All other users are prohibited from accessing those functions through a combination of programmatic and system level access control mechanisms. An example of one such system mechanism is that 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.</p> <p>See the System Functions answer to question #2 for details on how this role-based access is granted by the CDX Help Desk or Program Office RMAM.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<p><b>15. Procedures to flag spurious credential use</b></p>	
	<p><b>Business Practices:</b></p> <p>The CDX Electronic Signature Agreement (ESA) requires the user to notify the CDX Help Desk or the sponsoring Program Office in the event that they receive notification of a submission that they did not perform.</p>

The CDX Security engineers perform a weekly review of all security-related log files on the system (audit logs, CAM 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 order to further protect against a credential compromise going undetected by the original user, some information provided during the user's registration process cannot be changed by anyone who has gained subsequent access to that account. One example of such an item is the user's registered email address. The system notifies the originally registered account owner of all account-related actions using this out-of-band email address, i.e., actions such as a password change, phone number change, or secret answer change. The user can request a change to this email address only through contact with the CDX Help Desk – a process during which their identity information and secrets are explicitly challenged.

**System Functions:**

CDX e-Signature and PKI Enabled Applications: During the 20-5-1 security question/answer document signing procedure, the user is prompted to supply their user account password and the secret answer to one of their five chosen 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 condition, similar to the standard actions taken for a standard user authentication failure. An account lock-out condition will automatically result in an out-of-band e-mail being sent to the registered email address for that User ID and a message will be placed into that user's MyCDX in-box. The message indicates that the locked-out user must contact the CDX Help Desk and provide identity-proofing information in order for the CDX Help Desk to re-enable the user account. Upon re-establishing the user's identity, the CDX Help Desk will reset the user account password and 20-5-1 question/answer set to a temporary one-time-use value in order to allow the properly identified user to login and re-enter these items.

CDX PKI Enabled Applications Only: In addition to the above, if the associated CDX User ID does not match the CDX User ID associated with the X.509 certificate, CDX will reject the user's attempt to use the certificate in the signing process. This condition is also noted in the CDX audit logs.

	<b>Supporting Documentation (list attachments):</b>
--	---

**16. Procedures to revoke/reject compromised credentials**

	<p><b>Business Practices:</b></p> <p>CDX e-Signature and PKI Enabled Applications: When notified of a compromised pin/password credential the CDX Help Desk will immediately lock the user account associated with that credential using the CDX Help Desk tool. The user will then have to undergo another round of identity proofing by the CDX Help Desk in order to reset their pins/passwords and unlock their account.</p> <p>CDX PKI Enabled Applications <u>Only</u>: In addition to the above, when notified of a certificate with a justifiable reason requiring revocation (i.e., key compromise, CA compromise, affiliation change, superseded, termination of employment, cessation of operations, etc.), the CDX Help Desk will log in to the CA-sponsored web site and request revocation of the compromised certificate using their web-based tool and the certificate serial number assigned to that user. Alternatively, the CDX Help Desk can call the CA’s Certificate Revocation Hotline. This will result in the certificate serial number being added to the CA’s certificate revocation list – meaning that subsequent attempts to use the certificate will be rejected by the CDX CAM validation process (as discussed in question 13C).</p>
	<p><b>System Functions:</b></p> <p>See Question 13-C for a discussion on the rejection of compromised credentials by the CDX system.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

**17. Confirmation of signature binding to document content**

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>Upon receipt of signed document, the CDX system performs the following actions:</p> <ol style="list-style-type: none"> <li>1) Calculation of the current message digest (hash) value of the received document using the standard SHA-1 algorithm</li> <li>2) Decryption of the received signature hash using the supplied public key in order to obtain the original document hash value at signing time</li> <li>3) Comparison of the current hash value with the original hash value</li> </ol> <p>CDX performs this signature validation (currently using the COTS product ASPEncrypt) upon the uploading of the signed submission file to the CDX web servers. Failure to pass the signature validation results in a "submission failure" out-of-band e-mail being sent to the registered email address for the submitter. This message will be also placed into the submitting user's MyCDX in-box. This condition (signature validation failure) is also noted in the CDX audit logs.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<b>Copy of Record</b>	
<b>18. Creation of copy of record (See 18a through 18e)</b>	
<b>18a. True and correct copy of document received</b>	
	<p><b>Business Practices:</b></p> <p>Please see #9 for a description of the CDX COR.</p>

	<p><b>System Functions:</b></p> <p>While in transit, the integrity of the submission document is protected through the mechanisms of the SSL HTTPS connection (see question#8).</p> <p>The CDX system will validate each user-signed submission document upon receipt (see question#13 for methods used). In cases where the submission document is not digitally signed by the submitter, 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 (1024-bit minimum key length). This signed message digest, along with CDX's public key, would be stored with the document in the COR in order to provide for subsequent detection of changes to the original submission document content.</p> <p>The CDX Server certificate is stored in an OS-protected key store that does not allow subsequent exportation of the installed key. Applications which retrieve the private key must be granted system-level access and can only reference/obtain the key through OS-level API functions. Administrators and others with server level access cannot directly access/view/obtain the key store or its contents. The CDX server certificate is replaced bi-annually, as part of an ongoing CDX system maintenance procedure.</p> <p><b>Supporting Documentation (list attachments):</b></p>
<p><b>18b. Inclusion of electronic signatures</b></p>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>CDX retains document signature information and related public keys whenever a submission document or any of its related documents (such as those containing submit-time metadata collection</p>

	<p>items) are stored. Please see Question #9 for a description of the contents of the CDX COR.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<p><b>18c. Inclusion of date and time of receipt</b></p>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>Date and time of submission receipt is retained as a standard part of the CDX COR. Please see Question #9 for a description of the contents of the CDX COR.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<p><b>18d. Inclusion of other information necessary to record meaning of document</b></p>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p>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 (See the description for item #2 under question #9 for a complete discussion of COR content).</p>

	<b>Supporting Documentation (list attachments):</b>
<b>18e. Ability to be viewed in human-readable format</b>	
	<b>Business Practices:</b>
	<b>System Functions:</b> See Item 9b for more information on how the COR is provided in a human-readable format.
	<b>Supporting Documentation (list attachments):</b>

<b>19. Timely availability of copy of record as needed</b>	
	<b>Business Practices:</b>  Each Program Office application owner specifies the rules related to the granting of access to the CORs for their application. The original submitter and the CDX Help Desk are always granted access, with other supporting groups (such as reviewers and approvers) being granted access according to their role and/or group relationship to the submitter.  The CDX Help Desk is supplied with tools to manually retrieve and provide information concerning the copy of record within 1 business day upon request from the Submitter and/or Program Office (upon suitable identity proofing). The requestor will need to provide the transaction ID and/or other identifying information related to the submission of interest. The submitter's user ID and submission time period can be used when the transaction ID is unknown.

**System Functions:**

CDX generates the COR during the submission process and immediately generates a notification to the user of this action (see question 9A). Users will be able to view the COR online immediately upon their receipt of the submission notification message.

The COR is also available at any time following submission through the transaction history dialog. This dialog is invoked from the user's MyCDX home page after user login to the CDX system. The submitter (or other authorized users) can use this dialog at any time to view and download all data content related to a submission.

CDX will allow submitters to search for CORs using the transaction history dialog using at least the following fields:

1. Date Range

The CDX Help Desk and Authorized Program Office users will be provided with additional transaction history dialog search criteria, such as Application Name, User Id, Transaction ID, User Affiliation Code, etc.

If the COR contains only the original submission document, the document is available as soon as the submitter submits the data. If any COR item needs to be "decrypted and re-encrypted" or "processed and supplied" by the receiver and/or a backend application, the COR will be available to the submitter as soon as the receiver and/or the backend application sends it back to CDX in the appropriate form – whereupon it will be associated with the original submission materials and made available as described above.

The CORs will be searchable and viewable for the entire length of time for which they are maintained on CDX (see question 20).

	<b>Supporting Documentation (list attachments):</b>
--	---

<b>20. Maintenance of copy of record</b>	
--	--

	<p><b>Business Practices:</b></p> <p>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 <i>CDX Separation of Duties Guide</i>. This 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. All CDX personnel with access privileges to the production environment are required to have at least a Minimum Background Investigation (MBI) clearance check.</p> <p>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 <i>CDX Contingency Plan</i>.</p> <p>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 unless otherwise specified by the Program Office.</p>
	<p><b>System Functions:</b></p> <p>At the completion of the creation of the COR, CDX computes a SHA-1 hash value of all the items that make up the COR. This hash value is then 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.</p> <p>Other COR creation actions and related information (e.g., User IDs, file names, document signatures,</p>

etc.) are also automatically captured by the system and written to CDX audit logs. Once per day the CDX system copies these log files to a separate server and applies a separate signature to prevent/identify tampering with log file content. This process (call UATSign) provides an additional independent means of validating the integrity of COR content as maintained on the database servers with that information captured to/provided by the audit logs.

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-line storage.

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 file BLOBs that have passed their expiration period (based on submission date/time stamp). Non-BLOB objects that make up the COR 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. Data BLOBs remain accessible for recovery, as necessary, through historical backup tapes.

**Supporting Documentation (list attachments):**

Attachment 9 – CDX Separation of Duties Guide

Attachment 10 – CDX Contingency Plan 04-28-06.doc (Available upon request)