CROMERR System Checklist	
Item	
Registration (e-signature cases only)	
1. Identity-proofing of registrant	

Business Practices:
Cross-Media Electronic Reporting Requirements (CROMERR) 3.2000(b)(5)(vii)(C) specifies receipt of a signed Subscriber Agreement proves a registrant's identity. eSE-Verify uses an Electronic Subscriber Agreement (ESA) for this purpose, specifically tailored to the IDEM e-Sample Entry (eSE) application and hereafter referred to as the eSE ESA.

Standard ESA requires the Registrant's organization's Authorizing Official to acknowledge performance of the following duties to verify registrant has a valid identification (ref NIST 800-63):

1. Verify registrant possesses a valid current primary Government Picture ID that contains the registrant's photograph and either address of record or nationality (e.g. driver's license or passport).
2. Compare photograph in Government Picture ID to registrant and record ID number and issuer as well as Registrant's address and Date of Birth, as it appears on the Government Picture ID.
3. Keep a record of above information for a minimum of five years after registrant's employment termination or change in position.

Attachment 1 shows the draft eSE ESA.

A. eSE-Verify Registration Process:

1. Registrant completes eSE-Verify's online profile
2. Registrant downloads and prints hardcopy eSE ESA form containing information just entered
3. Registrant signs eSE ESA form
4. Registrant's organization's Authorizing Official verifies registrant's identify and signs eSE ESA form
5. Registrant mails hardcopy eSE ESA to eSE-Verify System Administrator

B. eSE-Verify System Administrator Verification Process:

1. Signed eSE ESA received by the eSE-Verify System Administrator must meet the following conditions:

a. Have no alterations that materially change the meaning and/or substance of the document have been accomplished beyond those necessary for the registrant, the organization's authorizing official and/or other company personnel to complete the document.
b. Be complete (excluding sections reserved for official IDEM use).
c. Contain registrant's handwritten signature.
d. Contain registrant's organization's Authorizing Official's handwritten signature.

2. eSE-Verify System Administrator contacts registrant's organization's Authorizing Official and/or employer by telephone, and verifies the information supplied in the hardcopy eSE ESA form .The eSE-Verify System Administrator verifies:

   a. eSE ESA completeness
   b. eSE ESA contains registrant's handwritten signature
   c. eSE ESA contains registrant's organization's Authorizing Official's handwritten signature
   d. Registrant's employer
   e. Registrant's authorization level
   f. Registrant's ability to serve as a signatory, and, if so, if authority has been delegated

3. The eSE-Verify System Administrator maintains verified eSE ESA in a paper filing system until it may be scanned (e.g. as .pdf page) for storage within existing IDEM document management capability.

4. IDEM currently retains eSE ESAs for all signing credentials for a minimum of five years after account deactivation.

System Functions:
eSE-Verify presents each registrant with a link to

1. Download and print the eSE ESA
2. Instructions for completing it
3. Follow-up actions the eSE-Verify System Administrator will take on receipt of the eSE ESA

eSE-Verify creates a registrant record to store information supplied by the registrant.

eSE-Verify creates records to store information specific to eSE-Verify Administrator follow-on activities (the information presented to the Administrator in on-line checklists that must be completed before the Administrator can grant registrant access to eSE and/or grant signatory/submission capability (where requested).

Supporting Documentation (list attachments):

The agreement includes language, in the first person, stating registrant

1. Agrees to:

   a. Protect the account and password from compromise, not allow anyone else to use the account, not to attempt to use or create automated log-in scripts for his/her electronic signature credentials, and not share the password with any other person;
   b. Change the password should it become known to any other person;
   c. Promptly report to IDEM authority (e.g. eSE-Verify System Administrator) any evidence of the loss, theft, or other compromise of the account or password not later than one business day;
   d. Have certifying authority notify IDEM authority (e.g. eSE-Verify System Administrator) in writing if of termination of employment or reassignment of Certifier status for the organization – with notification to IDEM authority occurring as soon as this change occurs;
   e. Report any evidence of discrepancy between submission file and what eSE application receives;

2. Understands that he/she is legally obligated and responsible for the use of his/her

	electronic signature as he/she would be by a handwritten signature in submitting electronic documents.
1a. (priority reports only) Identity-proofing *before* accepting e-signatures	
	Business Practices: For an eSE-Verify registrant to be granted security/signatory credentials, registrant must complete the on-line registration process (discussed in Item 1, above), complete an ESA, and have his/her identity verified through rigorous identity-proofing procedures conducted by an eSE-Verify System Administrator. The eSE-Verify System Administrator may not grant signatory authority to an eSE-Verify registrant prior to: 1. Receiving registrant's completed eSE ESA and 2. Verifying it through telephone interviews with registrant's organization certifying official.
	System Functions: eSE-Verify will not enable a registrant's electronic signature device to sign electronic documents until registrant's eSE-Verify System Administrator receives and verifies the eSE ESA and demonstrates successful verification by setting the appropriate flags in eSE-Verify (application and database). The registrant's highest authorization level and signatory right for a given organization are explicitly stored in the eSE-Verify database. eSE-Verify grants authorization level(s) and/or signatory right if the following conditions exist in the eSE-Verify database: 1. Successful completion of identity-proofing process (i.e. checklists) 2. Appropriate enabling flags set to indicate highest authorization level 3. Signatory right indicated by flag in the database Registrant login attempt triggers above checks.
	Supporting Documentation (list attachments): See Attachment 1 Draft eSE Subscriber Agreement See Attachment 2 eSE-Verify Registration Process
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: N/A – see 1b-alt Subscriber Agreement alternative
	System Functions: N/A – see 1b-alt Subscriber Agreement alternative
	Supporting Documentation (list attachments): N/A – see 1b-alt Subscriber Agreement alternative

CROMERR System Checklist	
1bii. (priority reports only) Information or objects of independent origin	
	Business Practices: N/A – user 1b-alt Subscriber Agreement alternative
	System Functions: N/A – user 1b-alt Subscriber Agreement alternative
	Supporting Documentation (list attachments): N/A – user 1b-alt Subscriber Agreement alternative
1b-alt. (priority reports only) Subscriber agreement alternative	
	Business Practices: CROMERR 3.2000(b)(5)(vii)(C) specifies receipt of a signed Subscriber Agreement as proof of registrant identity. eSE-Verify uses the eSE ESA for this purpose. Before eSE-Verify registrant is issued signatory/submission credentials, registrant must complete the on-line registration process (see Item 1), complete the eSE ESA, and have his/her identity verified through rigorous identity-proofing procedures conducted by the eSE-Verify Administrator. To grant signatory/submission authority to an eSE registrant, eSE-Verify Administrator must receive: 1. eSE ESA completed by the registrant and 2. Verify registrant's signed eSE ESA through telephone interviews with officials of registrant's organization. Note: Signatory/submission authorization (which gives registrant capability to sign/submit files is determined by the organization's authorizing official who communicates the need for the registrant to have this authorization level to the eSE-Verify System Administrator and confirms this authorization request during the identity-proofing process and discussions between eSE-Verify System Administrator and organization's authorizing official(s).
	System Functions: Registrant completes his/her part of eSE-Verify's online profile. eSE-Verify provides the name and mailing address of the eSE–Verify System Administrator to which the registrant's organization's authorizing official mails the signed eSE ESA. Registrant Profile The online eSE-Verify registrant profile requires the following information: 1. Email address (this must be a unique email address within system and serves as registrant's User ID for eSE Verify; if new registrant enters an Email USer ID that has previously been used, eSE Verify provides this rejection message: Your Email Address acts as your User ID and the one you entered is already in use. Please provide a different Email (User ID). 2. Full name (First Name, Middle Initial (optional), Last Name) 3. Mailing address (Street, City, State, Zip) 4. Telephone Number 5. Organization for which registrant is employed and on whose behalf access is desired

	Supporting Documentation (list attachments):
2. Determination of registrant's signing authority	
	Business Practices: IDEM is responsible for establishing and documenting policies and procedures to: 1. Determine the accuracy of registrant information 2. Verification of registrant information 3. Determine, for the each organization associated with the registrant, the following: a. Organization(s) registrant is authorized to represent b. Appropriate authorizations c. Appropriateness of registrant's signatory/submission authority d. Granting, if appropriate, registrant's signatory/submission authority In the eSE ESA, each registrant's organization's authorizing official attests that eSE registrant is authorized to represent the organization and whether or not the registrant has signatory authority on behalf of the organization. A Sponsor Letter from the organization may be required attachment to the eSE ESA. The Sponsor Letter is on organization letterhead and must include the same attestations contained in the eSE ESA and the handwritten signature of the same authorizing official signing the eSE ESA. The registrant mails the completed eSE ESA and Sponsor Letter to the eSE-Verify System Administrator who then follows the standardized verification and identity-proofing procedures described in Item 1. eSE-Verify System Administrator maintains verified eSE ESA and Sponsor Letter in a paper filing system until they may be scanned (e.g. as .pdf page) for storage within existing IDEM document management capability and storage policy. For example, the eSE ESA, Sponsor Letter, and any other verification/identity-proofing documentation will be retained for 5 years following deactivation of the associated signature device.
	System Functions: eSE-Verify uses a flag-based authorization system. A registrant is entered into the database initially without signatory/submission authority flag enabled; access to signatory/submission authority is only activated when verification and identity-proofing requirements are complete. Registration processes for eSE are executed using eSE-Verify's on- line interface. eSE-Verify provides a registrant the necessary instructions and forms for: 1. Registering for access to eSE (online Registrant Profile page) 2. Downloadable eSE ESA form that is to be filled out and mailed to eSE-Verify System Administrator (for registrant to obtain signatory authority, if appropriate, on behalf of the organization) eSE-Verify enables creation of registrant's initial account by setting Account Active flag to Y; However, a registrant cannot sign for or submit a file until eSE-Verify System Administrator sets registrant's signatory authority flag to Y. Once registrant fills out eSE-Verify online registrant profile, prints and signs the eSE ESA, and registrant's organization's Certifier (authorizing official) has signed and mailed form to eSE-Verify System Administrator; and once eSE-Verify System Administrator goes through appropriate identity proofing procedures, eSE-Verify System Administrator activates registrant's signatory authority flag by setting it to Y. The eSE-Verify System Administrator has capability to grant, deny

	or revoke access to eSE and, if necessary, change signatory authorization.
	Supporting Documentation (list attachments): See Attachment 1 Draft eSE Subscriber Agreement See Attachment 2 eSE-Verify Registration Process
	CROMERR System Checklist
	3. Issuance (or registration) of a signing credential in a way that protects it from compromise
	Business Practices: eSE-Verify supports e-signature credentials, the specific component that dynamically accepts and verifies registrant's identity credentials (e.g. Email User ID/Password). Registrants must acknowledge adherence to the following policy in order to protect e-signature credentials: 1. Avoid constructs like personal name or birthday, child's or pet' name,). 2. Password needs at least eight characters and must be a mix of numbers and upper/lower-case letters. 3. Protect password by: a. Not sharing the password with anyone b. Memorizing them so there is no need for external storage c. Not allowing it to be written into computer scripts for automated login purposes. 4. Promptly report loss, theft, or other compromise of the user account password to the eSE-Verify System Administrator. 5. Promptly notify eSE-Verify System Administrator if the registrant ceases to represent the submitter organization. eSE-Verify's e-signature credentials include a set of protected questions/answers specific to each registrant and that are associated with each registrant's account profile. Twenty questions are stored, with five questions randomly selected for presentation after the registrant enters the online profile information. eSE-Verify stores registrant responses to the five questions. One of the five questions is then randomly selected and presented for response during the file submission process. Use of a randomly selected user-specified challenge question is known as the 20-5-1 security question/answer technique.
	System Functions: eSE-Verify provides several ways to securely issue signing credentials. The signing credential is the combination of registrant/account holder's Email User ID, hashed Password and the randomly generated (one of five) challenge question and hashed answer 1. Secure Socket Layer (SSL) connections - registrant accesses eSE, hosted on IDEM's server, via Secure Socket Layer (SSL) HTTP sessions (HTTPS) (SSL v3.0 128 bits (IOT Standard) and TLS v1.0 256 bits as noted in Section 8) precluding unauthorized entities from accessing information exchanged between the registrant and the application during an active browser session. Negotiation of SSL version used for secure sessions is controlled through server configuration files. 2. Email User ID and Password - Email address must be unique within system because it serves as registrant's User ID for eSE Verify; if new registrant enters an Email USer ID that has previously been used, eSE Verify provides this rejection message: Your Email Address acts as your User ID

and the one you entered is already in use. Please provide a different Email (User ID).

eSE-Verify enforces compliance of the requirement for registrant's password to be between 8 and 20 characters, at least one uppercase character, at least one lower case character, and at least one digit, and no space allowed (and not the same as any previous password).

Email User ID is stored in the eSE-Verify database with password and is protected by:

a. Applying a one-way hash (SHA-256) to the password
b. Storing the resulting Hex value in the eSE-Verify database
c. Storing a creation date timestamp in the eSE-Verify database

Subsequent registrant logins are accomplished by comparing the one-way hash value of the session-specific registrant-supplied password with the hash value of registrant's most recently established password.

3. Password Expiration and Retention

eSE-Verify expires passwords every 90 days including these actions

a. Sends registrant whose password has expired an email notifying of password expiration along with reset instructions (10 days before 90 day expiration and day of expiration).
b. Retains all registrant's previously entered passwords to prevent password re-use.

4. Restrictions When Modifying Registrant Profile

Registrants can change account profiles; however, eSE-Verify has a static message warning the registrant that changing any of the mandatory fields of the online profile requires the resubmission of the ESA and for the eSE-Verify System Administrator to go through the identify proofing process again. Changing registrant profile information also results in a confirmation warning message (select Yes to confirm change or No to not continue with changes) where registrant must confirm understanding that profile change of any mandatory fields will result in deactivation of signatory authority and need to resubmit the eSE ESA. Once registrant makes a change to his/her profile, eSE-Verify System Administrator is notified via email that the profile is changed and account is locked.

Registrant (account owner) is also notified, via email, of all account profile changes – so that registrant is aware of any account changes – these should all be known to registrant but in case another party attempts to change registrant's profile, registrant will be aware of account changes. Thus the original owner of the registered email address will continue to receive account profile modification notifications, even in the event the account is compromised. If registrant needs to change email address (Email User ID), registrant needs to go through the eSE ESA process again. The account owner must restart the eSE ESA process and re-undergo the identity-proofing process. The original, established email continues as the email address for registrant notifications until the eSE-Verify System Administrator completes the additional identity-proofing and establishes registrant's new account. At that time, registrant's new email address becomes the email of record.

5. Use of Security Challenge Questions

During registration, eSE-Verify displays a list of twenty security challenge questions from which the registrant must select five questions to which he/she provides an answer. Registrant responds to the five questions and provides answer for each selected challenge question (referred to as 20-5-1 challenge question/answer technique). eSE-Verify rejects an answer if it is just numeric, with this message: The answer to each of your five security questions must be provided as text and may not be a numeric. If the registrant provides an answer to a second or subsequent security question that has already been used for one of the five security questions, it is rejected with this message:

The answer to each of your five security challenge questions must be unique.
The 20 candidate questions are listed in embedded Attachment 4 of this item. During the submission process, after submitter's User ID and Password have been authenticated, the electronic signature utility randomly selects/presents one of the five previously answered challenge questions for submitter to answer. If submitter answers first question incorrectly, the electronic signature utility excludes that question and randomly selects from the four remaining questions. This loop continues until submitter either correctly answers a remaining question (all incorrectly answered questions are excluded – so a challenge question can only be asked once) or answers the last/fifth question incorrectly. Should the submitter incorrectly answer the last/fifth question, the submitter's account is locked. eSE-Verify secures each answer by:

a. Retrieving registrant's Email User ID
b. Hashing and storing registrant-supplied answer (SHA-256) in eSE-Verify database
c. Storing creation date timestamp in eSE-Verify database

For submission of files with electronic signature, eSE-Verify uses combination of registrant/account holder's Email User ID, hashed Password and the randomly selected (one of five) question and hashed answer. That is, the signing credential is the combination of registrant/account holder's Email User ID, hashed Password and the randomly selected (one of five) question and hashed answer.

6. Log History of Signing Credentials, Submissions, Repudiations

a. A history of signing credentials is maintained in the database in table CMR Submission in eSE Verify database
b. See attachment 5 (CMR Submission table fields with description of each field). This table stores hashed signing credential, the submitter associated with the signed credential, and the date timestamp on which the submission was signed/validated.
a.c. History of signing credentials is kept until 5 years after deactivation of the signing credential.
d. When database and archive file storage are established, table and file containing signing credentials, original submission file, etc. are established without delete privileges. The database administrator with update authority for eSE-Verify database will also set up DB monitoring tool to log changes to records that have previously been created. These measures plus dual storage of the credential information with each storage location not accessible by the other administrator (e.g. eSE-Verify DB Administrator cannot update/delete file Archive File Storage and Server Administrator responsible for eSE-Verify file repository cannot update/delete DB records) precludes alteration/deletion as much as is reasonable.

Supporting Documentation (list attachments):

See Attachment 3 eSE-Verify Signature – Submission Process

Attachment 4. See embedded list of eSE-Verify CROMERR-Challenge Questions

eSE Verify
(CROMERR) - Challen

See Attachment 5. CMR_Submission table with descriptions of each field

CMR_SUBMISSION
table with description

4. Electronic signature agreement*	
	Business Practices: See Item 1b-alt Designated IDEM staff will either scan the ESA into Virtual File Cabinet (VFC) for record keeping and will treat them as "confidential" (only accessible by limited staff); and/or designated IDEM staff will store ESA as a "paper" file, also treated as "confidential" and stored locked container (only accessible by limited staff) to include a log of anyone checking in/out a file. IDEM plans to require every application to expire at the end of 3 years (similar to a compliance period). Since each signed credential will be kept for 5 years after account deactivation, each application form will actually be kept for up to 8 years. When files are to be destroyed, IDEM Public Records staff maintain and apply procedures in the correct disposal of confidential files (to include ESAs).
	System Functions: eSE-Verify's registration system lets registrants download and print the eSE ESA either during the registration process or during existing registrant account profile maintenance. Subsequent processing of the eSE ESA is handled by business practices outlined in Item 1b-alt and this section.
	Supporting Documentation (list attachments):

CROMERR System Checklist
Signature Process (e-signature cases only)

5. Binding of signatures to document content	
	Business Practices: eSE-Verify supports use of eSE-Verify-specific account information and the electronic signature utility developed collaboratively by IDEM and US EPA (including use of 20-5-1 method challenge question) to authorize creation/use of electronic signing credential at time of file submission. See Item 3.6 System Functions for description regarding separation of server file repository and DBA functions. Dual storage of the credential information in database and server file repository with each storage location not accessible by the other administrator (e.g. DB Administrator does not have access to Archive File Repository and Server Administrator does not have access to DB records) precludes alteration/deletion of signing credentials as much as is reasonable.
	System Functions: 1. Submission File The Submission File is an XML document containing submitter's content (sampling results) at the time of submission and the signing credential (as described in Section 3) (in a zipped file). Submitter has already viewed (in human readable format) the contents of the batch file being submitted. The HTML for each submission is archived separately in an electronic file system as well as in database table CMR Submission in eSE Verify database. See attachment 5 (CMR Submission table fields with description of each field). This table stores hashed signing credential, the submitter associated with the signed credential, and the date timestamp on which the

submission was signed/validated.

2. Submission Receipt

A Submission Receipt (SR) is created for each submission at the time of the submission. The SR is an XML document containing additional data/metadata related to the data document and is tightly coupled to the copy of record (COR) submission. The SR includes:

a. Document Submission ID (submission packet for eSE, globally unique ID)
b. Submission source: eSE
c. Submission type (e.g. eDWR)
d. Submission document type: XML
e. Submission date and time
f. Submitter account Email User ID
g. Submitter full name
h. Submitter operating system and version of submitting device
i. Submitter browser and version of submitting device
j IP of submitting device
k. Certificate public key
l. SHA-256 hash of the submission

The COR contains:

a. Submission File
b. Submission Receipt (SR)
c. HTML file of submitter's content

eSE-Verify uses the electronic signature utility developed collaboratively by IDEM and US EPA to validate electronic signatures and bind them to documents, found at this location:

http://test.epacdxnode.net/cromerr/site/download.html

During the submission process, users are informed of the implications of review/certification/signing of submission file as described in Items 6 and 7. After user acknowledges these conditions, eSE-Verify downloads a client side control to the user's workstation and prompts user for current account password. This password, along with the current Email User ID from the eSE session management table is then hashed as described in Item 3 and compared to current Email 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 user has not walked away from the 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).

When a valid Email User ID/Password combination is provided, eSE-Verify randomly selects one of the five user-answered questions (during the 20-5-1 registration process) and requests that user provide the correct response to that question. See Item 3.5 System Function for explanation of how eSE-Verify randomly presents challenge question and excludes incorrectly answered questions. The current user-supplied answer is then hashed as described in Item 3.5 System Functions and then compared with the answer as originally recorded.

If the user-supplied answer to the 20-5-1 challenge is correct, eSE-Verify uses the client side control to create a 1024-bit public/private key pair generated by the EPA/IDEM CROMERR electronic signature utility. The public key from this process is stored in a X.509 signing certificate on the user workstation that also includes current user/session information. This X.509 certificate is signed by eSE-Verify server process using the eSE-Verify private certificate. (Public key is stored permanently with submission metadata in eSE-Verify database table CMR Submission,

column Submission_Receipt, for future revalidation if necessary.

A message digest for each submission document is created on the client by the client side control using an SHA-1 algorithm. The document is subsequently signed using an RSA key pair (public key/user's temporary private key). An SHA-256 hash of the signed document is then calculated. The temporary X.509 certificate, signed document, signature (encrypted document message digest) and the resulting SHA-256 value are submitted to the eSE-Verify server. eSE-Verify calculates an SHA-256 hash of the received signed document and compares the resulting value to the SHA-256 hash received from the client. Matching SHA-256 hash values ensure the signed document arrives intact. Non-matching SHA-256 hash values are treated as submission failures. Successful transmissions are inserted into the eSE-Verify database with a unique Submission ID (table CMR Submission, column Submission_Receipt). Storage of the SHA-256 hash in the eSE-Verify database facilitates quick, on-demand verification (via recalculation of the SHA-256 hash) that the Submission File has not been altered subsequent to initial insertion.

Supporting Documentation (list attachments):

See Attachment 3 eSE-Verify Signature – Submission Process

6. Opportunity to review document content

Business Practices:
The eSE file submitter reviews the complete content of the file to be submitted for electronic transmission. This step occurs prior to confirming the account as described in Systems Functions. The XML representation of the user's client web-browser content at the time of submission initiation is the document the user signs and submits.

When submitting the file, user's submission includes appropriate user attestations/certifications pertaining to ownership of the account associated with use of the electronic signature credential; and acceptance, understanding and explicit acknowledgement of authority to submit the file on behalf of the organization.

System Functions:
eSE-Verify presents submitter with a verification/confirmation page consisting of read-only statements and confirmation checkboxes. All certifications and affirmations are in first person and user must confirm prior to proceeding with submission. Read only statements include:

1. Certification statement that the submitter is the owner of the account he/she is using and s/he has protected the account and password and is in compliance with the eSE ESA.
2. Affirmation that the signatory is not aware of any compromise to his/her signature credential.
3. Agrees that providing the account password to sign the document constitutes an electronic signature equivalent to his/her written signature.
4. Certification/warning statement (in the first person) outlining legal implications of attaching their electronic credential device to submission materials.
4.5. Certification the submitter has authority to submit file on behalf of represented organization.

Confirmation checkboxes require the submitter to check the box before proceeding.

1. A checkbox indicating the submitter has read, understood, and acknowledged the certification statements and non-compromise affirmation. The submitter must place a check in the checkbox before the submission can be made (i.e. activate SUBMIT button).
2. A checkbox indicating the submitter has been given an opportunity to review all

	pertinent data associated with the submission. The submitter must place a check in the checkbox before the submission can be made (i.e. activate SUBMIT button). Submitter's acknowledgements/affirmations by entering a check in the checkboxes enable proceeding with next step of the submission (download of file to local computer). The attestation/warning statements that appear on the submission page the user electronically signs are included in eSE-Verify database table CMR Submission, column Submission_Receipt, for future revalidation if necessary. Hence, eSE- Verify can provide documentation showing these attestations were made in conjunction with signing and submitting a specific file.
	Supporting Documentation (list attachments): See Attachment 3 eSE-Verify Signature – Submission Process
7. Opportunity to review certification statements and warnings	
	Business Practices: eSE-Verify's confirmation page includes content outlined in Item 6; however, IDEM Drinking Water program office may elect to modify the specific text displayed by the system in the signature certification and warning statement(s)
	System Functions: Verification/confirmation pages or dialogs are presented to a user prior to affixing of electronic signature credentials, system acceptance of signed submissions. See Item 6 for the content that will, at a minimum, appear on verification/confirmation pages or dialogs and example verification/certification statements.
	Supporting Documentation (list attachments): See Attachment 3 eSE-Verify Signature – Submission Process

CROMERR System Checklist	
Submission Process	
8. Transmission error checking and documentation	
	Business Practices: In the unlikely event that errors occur, Indiana DEM will keep the erroneous/partial submission as status "repudiated" and request the Lab resubmit the file.
	System Functions: eSe-Verify uses only SSL-secured HTTP sessions (HTTPS). eSe-Verify supports SSL v3.0 128 bits (IOT Standard) and TLS v1.0 256 bits. These protocols ensure encrypted application data exchange between client and server. SHA-256 hash of submission file is computed on client machine (post signature-binding) and submitted with submission file. Prior to insertion into appropriate copy of record (on server), the system re-computes the SHA-256 of submission and compares it to client submitted - SHA-256 hash. Identical values ensure submission is received intact. Non-identical values result in failure of the submission file. In either case both submitter and eSE-Verify Administrator are notified via email of the status of the submission. Additionally, the user is notified in real-time by an appropriate dialog displayed at the end of the submission session. Each eSE submission and its success/failure is tracked in system audit logs that contain:

1. File name submitted to eSE
2. Submission document type (i.e. eDWR)
3. Submitting Email User ID
4. Submission Timestamp
5. Submission outcome (Success or Fail)
6. Globally Unique ID (if Success)

The integrity of submission files and/or data is additionally protected as follows:

A. Submitted documents are presented in XML format on the user's client browser at the time of signing.
B. The XML representation of the user's client web-browser content at the time of submission is the document the user signs, thus ensuring the user sees the document being submitted
C. Information in submission XML file used for the verification page comes from data already stored in the eSE-Verify database. No updates to this data are performed at any time during or after the submission process.
D. No alteration of the document content is made during transmission or after it is received.
E. Unaltered XML document is in Submission File. This assures that the Submission File contains the same data in the same format the user was given the opportunity to review (see Item 6).
F. For successful transmissions the signature (see Item 5) is provided to the user in email acknowledgement along with instructions to access the Submission File. The email allows the user to detect modifications to the submission. See Item 5.
G. It is computationally infeasible for the user to create a valid Submission File signature without eSE-Verify generated one-off public and private keys. This protects against users modifying the Submission File and attempting to claim the data were altered using eSE-Verify.
H. Signed Submission File validity can be determined using eSE-Verify 'one-off' public key (as generated by IDEM-US EPA developed electronic signature utility).
I. This assures that the eSE-Verify 'one-off' private key was used to sign the submission.
J. Post submission data hash can be recomputed, if needed, to compare against the original values and thus determine whether stored binary submission objects have been altered.
K. Submitter can review data during data entry, and prior to and after submission.

Supporting Documentation (list attachments):

9. Opportunity to review copy of record (See 9a through 9c)

9a. Notification that copy of record is available

Business Practices:

See Item 5 and 6 for Copy of Record (COR) content.

Users are notified of the availability or submission failure of the eSE COR through the System Functions described below. Notifications always contain at least a standard set of information; however, additional content can be specified for inclusion by each IDEM Program Office (PO).

System Functions:

eSE-Verify informs submitters of COR availability:

1. Automatic notification to the user's registered email address after each submission with:
    a. Success or failure of submission

b. Instructions on how to access COR

2. Users may check eSE-Verify COR submission status by
   a. Searching for successfully submitted COR's
   b. Listing all submitted COR's.

For information on how a user would view the COR see Item 9c.

Supporting Documentation (list attachments):

9b. Creation of copy of record in a human-readable format

Business Practices:

eSE receives submission files as XML formatted documents. The HTML file is an exact copy of the submitter's browser content (i.e. human-readable plain text source used to display XML file content) at the time of signing. A signatory authority can retrieve and display the signed document at any time, viewed exactly as it was presented to the submitter at the time of signing – in human-readable format.

System Functions:
COR submissions are XML documents and include the HTML and submission receipt. The HTML file is an exact copy of the user's browser content (i.e. human-readable plain text source used to display document content) at the time of signing. Source XML and HTML tags inherently provide data context. Thus, the user or appropriate system function is able to retrieve and display the signed document at any time for viewing exactly as it was presented to the user at the time of signing.

After a user has acknowledged all necessary certifications/affirmations and explicitly elected to sign and submit, the COR is created and stored/retained in the eSE-Verify database.

See Items 5 and 6 for information on what comprises a COR and the COR creation and submission processes.

See Item 9c for how users can search for, view and/or download the COR.

Supporting Documentation (list attachments):

See Attachment 3 eSE-Verify Signature – Submission Process

CROMERR System Checklist

9c. Providing the copy of record

Business Practices:

None.

System Functions:
eSE-Verify enables retrieval and display of Copy of Record (COR) in these ways for Registrants with signatory authority:

1. Search on Submission ID

2. Search on Status ("SUCCESS" is default but can also search on "ACCIDENTAL", or "REPUDIATED")
The stored HTML file (as part of the COR) is displayed via standard browser. eSE-Verify System Administrators may additionally specify Email User ID as part of search and download any eSE Submission File/Submission Receipt and view the HTML.

Submitters using eSE-Verify receive email notifications regarding their submissions with sufficient information to easily locate COR's.

See Item 10. (eSE Submission page informs submitter In the event it is necessary to repudiate a submission.) See section 3 of Item 10 language regarding repudiation of the COR,

Supporting Documentation (list attachments):

10. Procedures to address submitter/signatory repudiation of a copy of record

Business Practices:
Signatories should promptly repudiate any submissions for which they do not want to be held accountable. A variety of scenarios could occur where an eSE user with signatory/submission authority may wish to repudiate a Copy of Record (COR):

1. An authorized signatory did not submit the COR.

eSE users with signatory/submission authority who dispute a COR submission should contact the eSE-Verify System Administrator, who will obtain the submission data and associated metadata, the date/time of submission, the submitting Email User ID, audit logs, the public key, and the signature hash that were stored with the submission. That information, along with eSA ESA is used to establish the identity and authority of the submitter with respect to a particular submission.

If it is found that the authorized signatory did not submit the COR, it is assumed the user's signature credential has been compromised. In this situation, the user's account is immediately locked by the eSE-Verify DBA System Administrator and the disputed COR flagged as repudiated. See below for further actions the eSE System Administrator and user should take in this situation.

2. An authorized signatory claims his/her signing credential is compromised or used inappropriately OR a determination that a authorized signatory's signature device has been compromised

If an authorized signatory claims his/her signing credential is or has been compromised or if the eSE-Verify System Administrator has verified compromise, the eSE-Verify System Administrator immediately locks the user's account. The eSE-Verify System Administrator investigates to determine the extent of the compromise and whether any submissions need to be repudiated. The eSE-Verify System Administrator also investigates any situation where a user who receives an email indicating repudiation of an eSE COR reports not having taken that action. All documentation associated with investigation is kept for at least 5 years. All compromised CORs are flagged as repudiated by the eSE-Verify DB System Administrator. The user and the eSE-Verify System Administrator investigate how the account may have become compromised.

3. A submission is erroneous and/or was submitted accidentally

In general, authorized signatories are allowed to resubmit CORs (see Item 11), If the signatory needs to repudiate the COR, the COR and signatory's account will be treated in a similar fashion to the procedures outlined for unauthorized submissions and/or comprised signing credentials.

	Signatories should promptly repudiate any submissions for which they do not want to be held accountable. On receipt of information that a Submitter wishes to repudiate a submission, eSE-Verify System Administrator must verify identity of Submitter as well as the information to identify specific file(s) to be repudiated. The eSE-Verify System Administrator may access the eSE System Administration Telephone Identity Verification function where the Administrator enters a Registrant's Email User ID and after verifying the registrant's name and other contact information, can select the Registrant Challenge question link. This link uses the electronic signature utility's function to randomly present to the eSE-Verify System Administrator the first of the registrant's five pre-selected/answered challenge questions. The eSE-Verify System Administrator reads the question to the registrant over the telephone and enters the response the registrant verbally provides. Should the response be incorrect (including that it may be entered incorrectly by the System Administrator), the wrongly answered question will be excluded from the set of next four randomly selected registrant challenge questions, as described in Item 3.3. This loop continues until a question is correctly answered. If the fifth security question is not correctly verbally answered by registrant/correctly entered by System Administrator, the account does not automatically lock; but the registrant's identify is not considered verified.
	System Functions: A COR is never removed from the eSE-Verify database. eSE-Verify by design, has no on-line facility to repudiate submissions. If a submitter or other user wishes to repudiate a copy of record, s/he must contact the eSE-Verify System Administrator and make the request. The eSE Submission page informs the submitter that in the event it is necessary to repudiate a submission (e.g. to dispute a COR submission) or to report an accidental or erroneous submission, submitter should promptly contact the eSE-Verify System Administrator so this submission status may be updated appropriately. The authority to repudiate a submission is verified by the eSE-Verify System Administrator as well as with one of the user's security questions to ascertain identity. The eSE-Verify System Administrator may access the eSE System Administration Telephone Identity Verification function where the Administrator enters a Registrant's Email User ID and after verifying the registrant's name and other contact information, can select the Registrant Challenge question link. This link uses the electronic signature utility's function to randomly present to the eSE-Verify System Administrator the first of the registrant's five pre-selected/answered challenge questions. The eSE-Verify System Administrator reads the question to the registrant over the telephone and enters the response the registrant verbally provides. Should the response be incorrect (including that it may be entered incorrectly by the System Administrator), the wrongly answered question will be excluded from the set of next four randomly selected registrant challenge questions, as described in Item 3.3. This loop continues as described in Item 3.3 until a question is correctly answered. If the fifth question is not correctly answered, the account does not automatically lock; but the registrant's identify is not considered verified either. The submission repudiation is stored in column SUBMISSION_STATUS of table CMR Submission which triggers (1) an automatic email to the submitter [An eSE submission certified by your Email User ID with the following [Submission Receipt information] was repudiated on [date timestamp] and (2) an update in the file repository that the COR is in repudiated status. Both DB and File System repository data are maintained for standard minimum of 5 years). Additional rules for handling repudiated submissions may be determined at the IDEM Program Office level. See Item 3.6 System Functions for description regarding separation of server file repository and

DBA functions. Dual storage of the credential information in database and server file repository with each storage location not accessible by the other administrator (e.g. DB Administrator does not have access to Archive File Repository and Server Administrator does not have access to DB records) precludes alteration/deletion of repudiation information as much as is reasonable.

Verified COR repudiations are managed by eSE-Verify System Administrator on eSE-Verify's Submission Detail page. eSE-Verify System Administrator can lock user accounts as well as revoke and/or re-issue signing credentials.

Registrants with signatory authority may search for and download a COR they have submitted. eSE-Verify System Administrators may search for and download any eSE COR. Authorized signatories can view (read-only), search and download COR's, in part, to identify potentially suspect submissions and initiate repudiation-related communications.

Since all submissions, repudiated or not, are retained in COR data stores, submissions are accessible via appropriate COR search/view functions with status of each COR submission clearly indicated (i.e. active, repudiated, etc.). Retention of all COR submissions provides history for any submission period. The COR cannot be altered without detection as the hash will no longer match.

Supporting Documentation (list attachments):

11. Procedures to flag accidental submissions

Business Practices:
eSE users with signatory/submission authority who determine an erroneous or accidental submission was received by eSE may resubmit a corrected COR and /or repudiate the COR. However, the original submission is not deleted. Signatories should promptly repudiate any submissions for which they do not want to be held accountable.

If a document is erroneously submitted, submitting signatories can correct with a follow-up submission. In this situation, the submitter must contact the eSE-Verify System Administrator and have the erroneous submission flagged as such. The eSE Submission page informs the submitter that in the event it is necessary to report an accidental or erroneous submission, submitter should promptly contact the eSE-Verify System Administrator so this submission may be updated appropriately. eSE users with signatory/submission authority an accidental/erroneous submission to be marked as such must first have the action verified by the eSE-Verify System Administrator and secondly challenged with one of the user's security questions to ascertain identity. The eSE-Verify System Administrator also logs actions taken with regard to the repudiation request in appropriate system logs. If rights and identity are verified, the eSE-Verify System Administrator flags the COR as "accidental" (stored in column SUBMISSION_STATUS of table CMR Submission) and an automatic email is sent to the user. See Item 10 description of how eSE-Verify System Administrator performs over-the-phone identity verification using Registrant's Email User ID and registrant-provided answer to one of his/her five security questions.

Exact rules for handling erroneous submissions are determined at the IDEM Program Office level; however, at the very least, signatories of record are notified of the erroneous submission via an email sent to the signatory's registered email address.

eSE-Verify retains all submissions rendering them accessible via appropriate COR search/view functions with status of each COR being identified (i.e. active, accidental, etc.)

Retention of all COR submissions provides history for any submission period. A replacement,

clearly marked as "accidental", is an option that may be exercised according Program Office (PO) specific direction. Discussion of retention of COR submissions in Item 10 applies to this item. The COR cannot be altered without detection as the hash will no longer match.

If the signatory wishes to repudiate a submission (not the advised approach for erroneous submissions), the user must contact the eSE-Verify System Administrator. See Item 10 Business Practices and System Functions for detailed description of the repudiation process.

System Functions:
eSE-Verify provides several ways to prevent accidental submissions:

1. Submitters review submission content prior to submission.
2. Submitters confirm their intent to submit by providing their Email User ID, password and answer a user-specified security question.
3. Submitters are sent an email after every submission.
4. Submitters can review previously submitted COR's

eSE-Verify System Administrator can set Submission Status Flag to Accidental.

Supporting Documentation (list attachments):

CROMERR System Checklist

12. (e-signature cases only) Automatic acknowledgment of submission

Business Practices:

In the event email referenced below in System Functions is not deliverable, the IDEM eSE-Verify System Administrator follows up within 2 business days by contacting the submitter at his/her telephone number and/or the contact information of the Certifying Authority on the ESA. Should the System Administrator determine the email address is no longer valid (e.g. the person to whom the Email User ID belongs no longer works for the lab), the Email User ID account is immediately locked and the Administrator closes the account.

System Functions:
Upon successful submission/upload of documents, the submitter is presented with a message containing:

1. Confirmation of successful binding of the signature device.
2. Confirmation of successful uploading of document(s) through eSE-Verify.

Additionally, an immediate email notification is automatically sent by eSE-Verify to submitter's registered email address, including:

1. Email User ID used with submission
2. Date/Time of the submission
3. SHA-256 signing hash (can be used to compare to COR SHA-256 signing hash)
4. Other information related to the submission

The following email information is logged in eSE-Verify log files:

1. Submission document type (eDWR)
2. Email User ID
3. Submission Timestamp
4. Globally Unique ID
5. Sender email address
6. Recipient email address

7. Email body text content

Should the submission not be accepted, an email is sent automatically to the submitter: The submission was not accepted. Please contact eSE-Verify System Administrator to determine source of submission failure and resolve the issue.

See Item 3.6 (also referenced in Item 5.2) regarding Log History of Submissions including that documentation is maintained for minimum of 5 years.

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:

None

System Functions:

eSE-Verify compares the hashed forms of user-supplied password and answer to the challenge question provided during the signing process to the hashed forms of the user's password and the user's response to the challenge question stored in eSE-Verify database.

For 20-5-1 challenge question/answer, eSE-Verify determines the certificate issuer information contained in the temporary submission-signing X.509 certificate matches the official eSE-Verify signing certificate. If the issuer information is incorrect, the submission is rejected and an email will be sent to the registered email address for the submitter and the condition is also noted in the eSE-Verify audit logs.

See Item 3 for how eSE/eSE-Verify securely issues and protects Email User ID/Passwords.

See Item 5 for how eSE-Verify creates the temporary X.509 certificate for Email User

ID/Passwords

Supporting Documentation (list attachments):

13b. Determination of credential ownership

Business Practices:

None

System Functions:
eSE-Verify compares the hashed forms of user-supplied password and answer to the challenge question provided during the signing process to the hashed forms of the user's password and the user's response to the challenge question stored in eSE-Verify database.

For the 20-5-1 challenge question/answer, eSE-Verify validates that Email User ID contained in the signature matches the submitter's eSE-Verify Email User ID as stored in eSE-Verify database. If the information does not match, the submission is rejected and an email will be sent to the registered email address for the submitter and the condition is also noted in the eSE-Verify audit logs.

See Item 3 for how eSE/eSE-Verify securely issues and protects Email User ID /Passwords. See Item 5 for how eSE-Verify creates the temporary X.509 certificate for Email User ID /Passwords

Supporting Documentation (list attachments):

CROMERR System Checklist

13c. Determination that credential is not compromised

Business Practices:

The eSE-Verify System Administrator periodically reviews appropriate audit logs. Should the administrator suspect a possible account compromise, he/she follows established policies and procedures to lock the account and take appropriate follow-on steps (see Items 10, 11, 15, 16).

System Functions:
eSE-Verify provides Administrator and registrant lock-down functions for responding to credential compromise.

1. eSE-Verify Administrators have the capability to lock a registrant's eSE account.
2. Registrant also has capability to lock his/her own account if it appears credentials have been compromised. (Accounts not locked at the time of submission provide evidence that administrators and registrants believe a credential is not compromised at the time of submission.)

Further, eSE-Verify features the the 20-5-1 security question/answer assurance of the IDEM-US EPA developed electronic signature utility, where the signing instrument is a one-time-use-only X.509 certificate. This temporary certificate is only generated after prompting registrant for account Email User ID/Password and the answer to one of the five selected security questions. The hashed values of the current user-supplied Email User ID/Password and the answer to challenge question are then compared to the original hash values stored with eSE-Verify 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 in the eSE-Verify audit logs.

See Item 3 for specifics regarding user account, Email User ID /password and answer to challenge question.

Supporting Documentation (list attachments):

14. Signatory authorization

Business Practices:

See Item 2 for processes eSE-Verify System Administrators follow to grant signatory authority to eSE registrants. IDEM Program Offices (PO) are responsible for specific requirements over and above these to determine a registrant's signing authority.

System Functions:
eSE-Verify has a System Administrator role that can grant the a registrant's account credentials to be used for signatory purposes on behalf of the organization the registrant account represents. The name of the Organization and the name of Organization Authorizing Official (First Name, Last Name and title) is stored in the eSE-Verify database

Registrant's access to eSE and eSE signatory/submission function is checked at run time, prior to permitting access to the application. Registrant's Email User ID and Password are verified against signatory information stored in eSE-Verify database.

Supporting Documentation (list attachments):

15. Procedures to flag spurious credential use

Business Practices:
The eSE-Verify System Administrator periodically reviews appropriate audit logs. Should the administrator suspect a possible account compromise, he/she follows established policies and procedures to lock the account and take appropriate follow-on steps (see Items 10, 11, 15, 16).

Administrators can potentially ascertain spurious credential use by identifying suspicious activities via semi-automated query functions against audit logs (e.g. Unix text mining functions, Splunk, etc.). These kinds of query functions/COTS tools provide metrics such as failed login attempts, repeated credential validation failures, etc. These tools, which are manually executed via the appropriate administrative interface, provide Administrators the ability to filter output on a variety of criteria (e.g. date range). Established protocol requires administrators to minimally execute these checks on a weekly basis covering the previous week's entries and periodic checks encompassing previous month, quarter and annual time spans; however, exact schedules are dictated by each Program Office (PO). Administrators can spot-check audit logs and are encouraged to do so.

IDEM Electronic Signature Agreement requires eSE Registrants to notify IDEM authority (e.g. the eSE-Verify System Administrator) on receipt of a notification of submission he or she did not perform and/or any other unauthorized use of his/her account credentials.

Registrants are allowed to alter their account profiles; however, the system requires the user to answer a challenge question (established at registration time, see below) prior to gaining access to their account profile. This helps ensure that the user established the original account in question and was properly vetted.

All user changes to an account profilerepresenting his/her organization immediately disable access to that user profile for the organization. The eSE-Verify System Administrator is notified via system function(s) of the change. The account owner is also notified, via email, of all account profile changes. Thus the original owner of the registered email address will continue to receive account profile modification notifications, even in the event the account is compromised. Since the system notifies the originally registered account owner of all account-related actions using his/her email address, spurious use of the user's credentials would be detected by the registered user. Account owner must undergo another round of identity-proofing before the eSE-Verify System

Administrator reactivates the account.

A change to the user's registered email is handled as a special case. The new email address is not used for notifications (i.e. the vetted email continues to be the email address utilized for user notifications), and the old Email User ID account is locked. eSE-Verify System Administrator completes the new identity-proofing and Registrant creates a new account with new email address as a new User – Organization account. At that time, the new email address becomes the email of record for the Registrant representing the Organization.

System Functions:
eSE-Verify System Administrators have the capability to lock a registrant's eSE account. An eSE-Verify registrant also has the capability to lock his/her own account if it appears credentials have been compromised. (Accounts not locked at the time of submission provide evidence that administrators and registrants believe a credential is not compromised at the time of submission.) eSE-Verify System Administrators can use the Apache logs to detect the following conditions that may indicate spurious use of user credentials

1. IP address and date/time of each originating login attempt is entered into eSE-Verify logs. Many login attempts over short period and/or from different IP address may point to spurious use and/or compromise.
2. Irregular and/or unusual submission patterns.
3. Frequent overlapping login attempts.
4. Submission notifications are automatically sent to registrant's email address. Receipt of notifications for submissions not initiated by registrant would indicate at least spurious use if not outright compromise.

Supporting Documentation (list attachments):

CROMERR System Checklist

16. Procedures to revoke/reject compromised credentials

Business Practices:
When notified of a compromised user credential the eSE-Verify System Administrator investigates as describe in Checklist Items 13 through 15 and is required to immediately lock the account associated with that credential if evidence suggests it has been compromised. The registrant will then have to undergo another round of identity proofing by the eSE-Verify System Administrator in order to reset the Email User ID/Password and/or unlock the account. In addition, the eSE-Verify System Administrator investigates all submissions during the time for which the account was believed to be compromised

System Functions:

When Submitter logs into eSE using unique Email User ID and Password, if Email User ID and Password do not match after four password attempts, submitter's account is locked out after fifth failed attempt. In a similar manner, Submitter's account is also locked if Submitter fails to correctly answer the fifth randomly selected challenge question during the submission process.

eSE-Verify System Administrators have the capability to lock a registrant's eSE account. Registrants also have capability to lock their account if it appears credentials have been compromised. (Accounts not locked at the time of submission provide evidence that administrators and registrants believe a credential is not compromised at the time of submission.) An eSE registrant with signatory/submission authority whose account is locked cannot sign/submit a file using eSE-Verify.

After lockout, the Email User ID attempting/failing to authenticate as well as the eSE-Verify System Administrator both receive the following email notification (1) for failed password: Account for [Email User ID] has been locked because of failure to enter the correct password on the fifth attempt. Please contact eSE-Verify Administrator to verify identity and unlock account. (2) for five failed challenge questions: Account for [Email User ID] has been locked because of failure to enter correct response for any of five security questions. Please contact eSE-Verify Administrator to verify identity and unlock account.

Only the eSE-Verify System Administrator has the authority to unlock a locked eSE account.

See Item 13c for eSE-Verify rejection of compromised credentials.

Supporting Documentation (list attachments):

17. Confirmation of signature binding to document content

Business Practices:

eSE-VErify submitters sign documents using the IDEM-US EPA developed electronic signature utility. The submitter must supply the registered Email User ID, Password and correctly answer a randomly selected user-selected challenge question associated with submitter's account.

System Functions:

The submission process is described in Item 5. As described there, eSE-Verify guarantees submission integrity by:

A message digest for each submission document is created on the client by the client side control using an SHA-1 algorithm. The document is subsequently signed using an RSA key pair. (public key/user's temporary private key). An SHA-256 hash of the signed document is then calculated. The temporary X.509 certificate, signed document, signature (encrypted document message digest) and the resulting SHA-256 value are submitted to the eSE-Verify server. eSE-Verify calculates an SHA-256 hash of the received signed document and compares the resulting value to the SHA-256 hash received from the client. Matching SHA-256 hash values ensures the signed document arrives intact. Non-matching SHA-256 hash values are treated as submission failures. Successful transmissions are inserted into the eSE-Verify database with a unique Submission ID. In summary

1. The current message digest (hash) value of the received document using the standard
2. SHA-256 algorithm is calculated.
3. Decryption of the received signature hash using the supplied public key is used in order to obtain the original document hash value at signing time
4. The current hash value is compared with the original hash value

If any part of the COR was altered, including the signature binding information, the new signature would differ from the original. Failure to pass the signature validation results in a "submission failure" email being sent to the registered email address for the submitter and the signature validation failure noted in eSE-Verify audit logs.

Supporting Documentation (list attachments):

See Attachment 3 eSE-Verify Signature – Submission Process

CROMERR System Checklist

Copy of Record

18. Creation of copy of record (See 18a through 18e)

18a. True and correct copy of document received

Business Practices:

See Items 5 and 9 for a description of eSE-Verify Copy of Record.

System Functions:

See Items 5 and 9 for the contents of the COR and the process used to assure it is a true and correct copy of the data. See Checklist Item 5, explanation that COR contains:

a. Submission File
b. Submission Receipt (SR)
c. HTML file of submitter's content

and the HTML (in human readable format) of the contents of the batch file submitted/certified by Email User ID. See Item 3.6 System Functions for description regarding separation of server file repository and DBA functions. Dual storage of the credential information in database and server file repository with each storage location not accessible by the other administrator (e.g. DB Administrator does not have access to Archive File Repository and Server Administrator does not have access to DB records) precludes alteration/deletion as much as is reasonable.

See Checklist Item 6: the attestation/warning statements that appear on the submission page the user electronically signs are included in eSE-Verify database for future revalidation and/or if eSE-Verify System Administrator can provide documentation showing these attestations were made in conjunction with signing/submitting the document.

While in transit, the integrity of the submission document is protected through the mechanisms of the SSL HTTPS connection (see Item 8).

See Checklist Item 10: COR cannot be updated to state the COR cannot be altered, as the hash will no longer match.

eSE-Verify validates each submission document (see Item 13).

Supporting Documentation (list attachments):

18b. Inclusion of electronic signatures

Business Practices:

None

System Functions:

See Items 5 and 9 for the contents of eSE-Verify Copy of Record (COR) and information on how the electronic signature is included in the submission.

eSE-Verify retains submission signature information and related public keys whenever a submission document or any of its related documents (such as those containing submit-time

	metadata collection items) are stored.
	Supporting Documentation (list attachments):
18c. Inclusion of date and time of receipt	
	Business Practices: None
	System Functions: eSE-Verify Copy of Record includes the date and time of the submission. See Items 5 and 9 for more information.
	Supporting Documentation (list attachments):
CROMERR System Checklist	
18d. Inclusion of other information necessary to record meaning of document	
	Business Practices: None
	System Functions: The COR contains: a. Submission File b. Submission Receipt (SR) c. HTML file of submitter's content The eSE-Verify COR contains all necessary information associated with the submission including tags and data necessary to display the content of the submission file. See Items 5 and 9 for more information on what the COR contains and associated metadata.
	Supporting Documentation (list attachments):
18e. Ability to be viewed in human-readable format	
	Business Practices: None

System Functions:

See Item 9b, Item 9c and Item 18d for information on how eSE-Verify Copy of Record is provided in human-readable format.

Supporting Documentation (list attachments):

19. Timely availability of copy of record as needed

Business Practices:

IDEM Program Offices determine rules and procedures for requesting and receiving a Copy of Record submitted via eSE-Verify. Access to an eSE-Verify COR is generally granted to:

1. eSE-Verify System Administrator
2. Other internal users authorized by IDEM Program Offices (PO)
3. eSE COR authorized submitters

System Functions:
eSE-Verify generates and stores the COR during the submission process. A notification is immediately generated and sent to the email address of the COR submitter.

See Item 9 for description of the parameters by which a COR can be searched.

eSE-Verify has COR search/view functionality by which a COR can be reviewed on-line and/or downloaded for offline review by user's with sufficient authority.

COR's will be searchable, viewable and downloadable for the entire length of time for which they are maintained in eSE-Verify (see Item 20).

Supporting Documentation (list attachments):

CROMERR System Checklist

20. Maintenance of copy of record

Business Practices:

Indiana State Information Technology personnel are functionally and physically separated into two groups. This separation helps prevent unauthorized access to/unauthorized manipulation of systems and/or data. Servers are in a secure location within Indiana Office of Technology (IOT) spaces. IDEM staff do not have access to them. Firewalls are set up for all servers to ensure only IOT system administrators are authorized access to manipulate systems and/or data. IOT administrators use standard intrusion/virus detection tools.

Infrastructure Personnel

1. The Indiana Office of Technology personnel maintain and service network hardware, operating environments and user access to/security for State information technology resources.

Application Personnel

1. The IDEM Office of Information Services personnel develop/maintain Agency applications, maintain/administer Agency application user security and maintain/administer Agency databases.
2. The IDEM Drinking Water Branch assigns eSE-Verify System Administrator to perform/mediate eSE-Verify identity-proofing and to administer registrant accounts.

System Functions:

eSE-Verify stores/retains the Submission file in eSE-Verify database Submission table and also within a separate configurable file folder. The eSE-Verify System Administrator will configure the file folder storage according to local conventions/requirements.

eSE-Verify stores/retains COR in the Submission table in the eSE Verify database. The distributed nature of the various COR copies makes it extremely unlikely tampering with the COR will go undetected.

Each eSE-Verify submission is stored in one database record of (Submission table) The following is a list contained in the Submission Receipt as referenced in Item 5, stored in this table:

a Document Submission ID (submission packet for eSE, globally unique ID)
b. Submission source: eSE
c. Submission type (e.g. eDWR)
d. Submission document type: XML
e. Submission date and time
f. Submitter account Email User ID
g. Submitter full name
h. Submitter operating system and version of submitting device
i. Submitter browser and version of submitting device
j IP of submitting device
k. Certificate public key
l. SHA-256 hash of the submission

eSE-Verify contains logs that could provide supplemental information to that stored in the COR.

3. Retention

1. COR's are retained according to the retention schedule established by IDEM for eSE submissions with a default retention of 5 years.

2. eSE-Verify logs are retained for as long as the CORs are retained (5 years).

Physical Security

Oracle databases are maintained on servers providing storage via [?]. Systems from which eSE and eSE-Verify are deployed employ automated database backup procedures that allows for rollback/recovery of database objects at nearly any point in time.

Backups

1. All IDEM database files are automatically backed up on magnetic tape daily (incremental), weekly (full), monthly (full), quarterly (full), and annual (full) schedule for offline storage.

2. A typical rotation schedule is observed in order to retain the ability to recover files to any point in time down to a granularity of one day. Annual backups are permanently stored

	off-site. 3. IDEM databases are included in the Indiana Office of Technology (IOT) Disaster Recovery Plan and are subject to a 6 hr / 7 day recovery period.
	Supporting Documentation (list attachments):