Common CROMERR Application Challenges: General Application Issues

1. Listing of Authorized Programs – 40 CFR § 3.1000

Common Issues/Deficiencies: The application does not identify the authorized state program to be amended or revised to allow e-reporting.

The state must identify the authorized program to be amended or revised. The authorized program must be identified in the *Federal Register* Notice announcing approval of the program revisions. If the applicable program is not accurately identified in the *Federal Register* Notice, then the revisions will not be approved for the correct program.

Example of Effective Approaches:

Applicants should clearly identify the state program(s) to be amended or revised, such as RCRA, CWA, CAA or other program designation. This is most commonly done on the application cover sheet. For applications that cover multiple reports under different authorized programs, the state should be sure that the indicated applicable programs cover all of the reports. For example, the application cover sheet for the Oklahoma Department of Environmental Quality Electronic Document Receiving System ("OK DEQ EDRS") indicates the name of the state program as RCRA in the name of Report 1 for their system as follows: "Report 1:

* Regulated Waste Activity Notification (RCRA)."

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS

For More Information:
cromerr@epa.gov

http://www.epa.gov/cromerr/

2. Identification of Each Report by CFR Citation – 40 CFR § 3.1000

Common Issues / Deficiencies: The application does not identify the CFR citation for each report received by the system or it does not identify them correctly. The state must identify the correct CFR citation for each electronic report received by the system. For priority reports, the correct CFR citations are identified in 40 CFR § 3.2000 Appendix 1 Part 3. The CFR citations will be listed in the *Federal Register* Notice announcing approval of the program revisions. If the CFR citations are incorrect, the program revisions will not be approved. Applications may also include planned future reports. By including planned future reports, if they are approved, the submitter can avoid the need to amend their application or submit a new application when their systems begin accepting them.

Examples of Effective Approaches: Applicants should clearly identify the correct *Federal Register* citation for each report received. This is most commonly done on the application cover sheet. For example, the cover sheet for the OK DEQ EDRS application indicates that the citation for their "Regulated Waste Activity Notification (RCRA)" report is 40 CFR Part 261.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS

3. Attorney General Certification Statement – 40 CFR § 3.1000(b)(1)(i)

Common Issues / Deficiencies: The application does not include a certification of sufficient legal authority to implement electronic reporting signed by the State Attorney General or a designee. The State Attorney General or a designee must certify that the state has sufficient legal authority to implement electronic reporting before the application can be approved.

Examples of Effective Approaches: Guidance and an example of a signed certification are available on the Application Tools and Templates page.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS

Common Application Challenges:
Issues Associated with CROMERR Checklist Items
Common Checklist Challenges/Solutions

1. (Item 1: Identity-proofing of registrant) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(vii)(C)

Common Issues / Deficiencies: No description of business processes for storing paper signature agreements (subscriber agreements).

Systems using the subscriber agreement alternative must store the agreements so they are protected from alteration and destruction for as long as there may be any enforcement interest in the signatures executed with the associated electronic signature device. Note that this item must be addressed only for reports that require an electronic signature, including priority reports, where the system requires a paper electronic signature agreement to be signed by users. This is most commonly used by systems using CROMERR checklist item 1.b.alt.

Examples of Effective Approaches:

Example approach used by the Indiana IDEM eAuth system (this information was provided under Item 2 and supporting documentation from the Indiana IDEM eAuth CROMERR Checklist):

SYSTEMS USING A SIMILAR APPROACH:

- Indiana IDEM eAuth.
- OK DEQ EDRS

The eA-AppAdmin ensures the signature agreement, the Sponsor Letter, and identity-proofing procedure documentation (if appropriate) are stored in a paper-based filing system until such time as all documents are scanned and the images stored in IDEM's Virtual File Cabinet (VFC) document management system. The VFC will rely on the FileNet document management software to provide the foundation functionality for capture, storage, and access to the documents. The VFC capture application, web application, and web portal will access the FileNet repository through the use of FileNet user accounts which have been set up with the necessary access controls to ensure secure input and retrieval of documents within the VFC. The quality assurance process for capture of documentation by the VFC will be accomplished through the implementation of thorough operational procedures implemented by IDEM staff. In addition, the VFC application contains several safeguards to allow for the assurance of quality and accuracy during the capture process. The signature agreement, Sponsor Letter, and identity-proofing procedure documentation shall be retained for a period of 5 years after being notified of the applicant's departure from his/her sponsoring organization by a company official.

Example 2 of Effective Approaches:

Example approach used by the EPA NetDMR system (this information was provided under Item 1 and supporting documentation for the EPA NetDMR CROMERR Checklist):

Paper copies of the NPDES permit with signature are received by the Regional Office responsible for permitting and will remain on file along with any delegation of authority as required by 40 CFR 122.22. EPA Regions with primacy for administering the NPDES program using NetDMR will also receive signed subscriber agreements from individuals requesting the ability to sign DMRs electronically for particular permits. Upon receipt of the subscriber agreement, the Regional Office will verify the permit limits and the signatures on the subscriber agreement through direct contact with the facility. The Regional Office will verify that the "Cognizant Official" is in the ICIS-NPDES database for every facility the user includes in the subscriber agreement and that has been verified by the Region. The Regional Office will retain a paper copy of the subscriber agreement on file according to item #1b-alt. Upon verification, the Regional Office will assign the appropriate level of access in NetDMR.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Texas NetDMR
- EPA CDX
- EPA NetDMR

2. (Item 2: Determination of registrant's signing authority) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(vii)

Common Issues / Deficiencies: Incomplete description of processes for determining a registrant's signing authority. Missing detail often includes:

- how the signing authority of registrants was verified
- where multiple verification methods are described, specification of which users are subject to verification and which methods of verification are used

There must be a specifiable process for verifying a registrant's signing authority. Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Examples of Effective Approaches:

Example approach used by the Texas NetDMR system:

TCEQ staff will use due diligence when processing signed Subscriber Agreements. TCEQ will, to the best of its ability, validate the information provided to assure accuracy and that it is appropriate for the requestor to be granted signatory authority for the specified permits. If needed, they will contact the facility to address the matter or may compare the authority stated on the agreement with previously emailed hard-copy reports. Once this review is complete, the TCEQ will assign the user's account the appropriate NetDMR signatory permission. Furthermore, periodic inspections by TCEQ field staff may include validation of the authorized facility representative who signed the subscriber agreement to evaluate compliance with signatory authority requirements. If circumstances indicate a claimed authority may not be appropriate, this will trigger an administrative review.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

3. (Item 3: Issuance (or registration) of a signing credential in a way that protects it from compromise) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(i)

Common Issues/Deficiencies: Incomplete description of security for signature devices such as passwords stored on their systems. Missing detail often includes:

- where the devices are stored
- who has access to them
- how they are protected from being altered or deleted
- whether they are encrypted (or hashed)
- if encrypted, what encryption techniques are used and how the encryption keys are protected

Signature devices must be stored on the system so that they are protected from compromise, tampering, and deletion. Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Example 1 of Effective Approaches:

Example approach using a public key infrastructure (PKI) certificate used by the OK DEQ EDRS system:

SYSTEMS USING A SIMILAR APPROACH:

- OK DEQ EDRS
- EPA CDX

The private key generated by the DEQ Certificate Authority Server (Microsoft Certificate Server) is required to utilize the certificate to sign a document. The private key is encrypted by the certificate authority server when it is generated, using industry standard PKCS methodology (128-bit RSA). When signatories wish to utilize the certificate to sign a document, they will be prompted for the password needed to decrypt the private key for use. Certificates issued by DEQ will not be usable with any software package that does not support private key passwords, as those packages will not be able to decrypt the key for use. This provides an added layer of security for the digital signature certificate by requiring both a valid private key and a password to decrypt that private key prior to use.

As an additional layer of protection, users must select and answer 5 knowledge-based questions from a list of 20. Each question and answer pair will be combined into a hash and stored on the server. Without the appropriate question and answer combination, the hash cannot be recreated, and authentication will fail. DEQ stores only the question selected and a hash of the question and answer combination. The SHA-256 algorithm will be used to generate the stored hash.

To obtain a certificate, users must submit a wet-ink signed Electronic Signature Agreement (ESA) form to DEQ. If the ESA is approved, DEQ will notify the applicant via email that the request has been approved and that the certificate package is available for download. To obtain the certificate, the user must click the hyperlink to the SSL-secured ERS portal that is provided in the email. Then, the user must log onto the ERS portal using the strong password provided at the time of request, and correctly answer two randomly selected (using the millisecond as the seed of the random function) out of the five questions. Note that to obtain the certificate, the requestor must log in using the hyperlink provided in the notification email, as this hyperlink contains a 32-character unique identifier (System Generated GUID) download key used to obtain

the certificate. The hyperlink takes the user to the portal login page and provides the server with redirection information (download key) to be used to access the certificate. The certificate package will then be available for download. Once the certificate is obtained, users must provide their private key password each time they wish to sign a document.

Example 2 of Effective Approaches:

Example approach using PIN/password used by the Indiana IDEM eAuth system:

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

The eAuth system supports e-signature credentials for use via the real-time input and validation of a user's eAuth Enabled Application (eA-EApp) identity credential. User access and information exchanged with the eAuth system and all eA-EApp's is performed over Secure Socket Layer (SSL) connections. Negotiation of the version of SSL used for secure sessions is controlled through server configuration files. At registration, users specify their selection of an eAuth/eA-EApp user ID and password. The eAuth/eA-EApp user ID is automatically entered on the signature agreement submitted by the user. Users must select a password that will not be easily guessed (e.g., names, children's names, birthdays), and passwords must be at least eight characters long and contain a mix of numbers and upper/lower-case letters. Compliance with this guideline is automatically enforced by the eAuth system. Users must adhere and must explicitly acknowledge adherence to strict policies governing access to an eA-EApp, including policies for password protection and reporting account compromise. Users must also select and answer 5 knowledge-based questions from a list of 20.

User IDs are stored in the eA-EApp registration/security database, and passwords are securely stored by applying a one-way hash (SHA-256) to the password, and storing the resulting Hex value, as well as a creation date timestamp, in the registration/security database. Upon subsequent logins, user authentication is accomplished through a comparison of the one-way hash value of the session-specific user-supplied password with the hash value of the most recently established password. To independently secure each knowledge-based answer, the system concatenates the user ID, question number and user-supplied answer, hashes (SHA-256) the concatenated value, and stores the Hex value of the resulting hash, as well as a creation date timestamp, in the registration/security database. Use of the eAuth/eA-EApp User ID in the hash computation ensures that the supplied answers are tied to a particular eAuth/eA-EApp account.

Users must answer a secret question to access their account profile. All user changes to an account profile for a facility immediately disable access to that facility. The eA-AppAdmin 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. The account owner must undergo another round of identity-proofing before the eA-AppAdmin will reactivate 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), until the eA-AppAdmin completes the new identity-proofing and re-enables the user's account. At that time, the new email address becomes the email of record.

4. (Item 3: Issuance (or registration) of a signing credential in a way that protects it from compromise) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(i)

Common Issues / Deficiencies: No description of requirements for password or PIN strength when this is being used as the signature device, or—if requirements are described—no description of how system enforces those requirements.

System must enforce requirements for PIN/password strength where this is being used as the signature device. Note that this item must be addressed only for reports that require an electronic signature, including priority reports, where the system requires a paper electronic signature agreement to be signed by users.

Examples of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

The password must be a strong password, at least 8 characters long and containing at least 3 of the following four types of characters: upper case, lower case, numbers, and punctuation. This password is created and validated for acceptability during the completion of the Electronic Signature Agreement Application online.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

5. (Item 5: Binding of signatures to document content) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(ii)

Common Issues / Deficiencies: No identification of encryption algorithms, where encryption was used to bind electronic signatures to submissions.

Electronic signatures must be bound to content of submissions, so that content cannot change without detection after the signature is executed. Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Examples of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

The digital signatures are created by the Windows Certificate Services server using 1024-bit encryption and the RSA algorithm.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

6. (Item 8: Transmission error checking and documentation) – 40 CFR § 3.2000(b)(1)-(2)

Common Issues / Deficiencies: No description of system functions or business practices for:

- documenting transmission errors
- notifying users or system administrators if transmission errors occur

The system must document any transmission errors, and have a process to address the errors.

Examples of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

Oklahoma DEQ will rely on the standard TCP/IP over Ethernet technologies, which the internet currently uses as the transfer mode for all data. In the event of a transmission error on a digitally signed document, the document content would change, which in turn would change the hash value, thereby invalidating the digital signature and the document. Further, all interaction with the ERS portal, from initial application for a certificate and upload account through submission and review of documents, is secured via SSL (v3.0). For any document submitted, regardless of the presence of a digital signature, the SSL underlying protocol stack would detect changes between the communication end points, perceive those changes as corruptions and invalidate the document (changes in the encrypted document will cause decryption to fail). Any transmission errors will invalidate the signed document, and will cause SSL protocol to fail, thereby causing the receiving process to fail. ERS itself does not receive invalid transmissions, as these are prevented by the underlying PKI infrastructure. Transmission errors and changes in transmissions are handled by the protocol stack on the server, and invalid uploads and transmissions are therefore not received by the ERS portal. The protocol failure itself is logged in the web server logs on the host server.

SYSTEMS USING A SIMILAR APPROACH:

- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

Documents that were originally sent by DEQ but no longer have the DEQ signature are treated as invalid and changed, and therefore are rejected. In addition, documents without a valid

signature from an accepted signatory are treated as invalid and rejected. Finally, if the signature on the document does not match the user currently logged onto the ERS portal, the document is treated as invalid and rejected. An email detailing the reason for rejection is sent to both the submitter and the ERS Administrator. A record of the invalid submission attempt is created and stored in Edoctus. In cases where an invalid document is received, that document is stored as part of the invalid submission record. A failure message will then be presented to the submitter indicating they must resubmit.

7. (Item 8: Transmission error checking and documentation) – 40 CFR § 3.2000(b)(1)-(2)

Common Issues / Deficiencies: No description of system provisions for transmission error prevention and detection, such as Secure Socket Layer (SSL). The system must be able to detect transmission errors.

Examples of Effective Approaches:

Example approach used by the EPA CDX system:

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.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR
- EPA SDWIS

8. (Items 10 and 11: Procedures to address submitter/signatory repudiation of a copy of record (COR) and procedures to flag accidental submissions) – 40 CFR § 3.2000(b)(1)-(3)

Common Issues / Deficiencies: Incomplete description of how system handles submitter/signer repudiation, including cases where submittal is claimed to be accidental. Missing detail often includes:

- how users can repudiate a COR or report an accidental submission
- how system administrators determine whether to designate a report as repudiated or accidental
- how users can update their submission or submit a revised report

Where submission corrections or complete resubmissions are allowed, the system must ensure that the original COR is saved or that an adequate log is kept of any changes made.

Examples of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

For documents requiring electronic signature, the signatory or another verified representative of the regulated entity may request repudiation after sending the signed submission. Users can request the repudiation online by selecting it from the list of submitted documents and clicking a "request repudiation" button or by contacting the ERS Administrator via phone or email. The ERS Administrator will notify the appropriate person in the division concerned for approval. If the division approves repudiation of the document, the ERS Administrator will mark the document as "Cancelled." Once a document has been marked as repudiated, the original submitter will receive an automated confirmation email from ERS. The submitter can then resubmit the document.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

9. (Item 12: Automatic acknowledgment of submission) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(vi)

Common Issues / Deficiencies: No description of procedures to prevent fraudulent changes to the e-mail address for automatic acknowledgments of submission. Missing detail often includes:

- how the e-mail addresses are established and changed
- whether an e-mail address could be changed in the same user session in which data was submitted

The system must have procedures to ensure that the e-mail address actually belongs to the registrant who is supposed to be receiving the acknowledgments. Allowing a user to change his/her email address in the same session in which data is submitted may allow fraudulent address changes.

Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Example 1 of Effective Approaches:

Example approach used by the OK DEQ EDRS system (this information was provided under Items 1 and 9 of the OK DEQ EDRS CROMERR Checklist, and not under Item 12):

SYSTEMS USING A SIMILAR APPROACH:

- OK DEQ EDRS
- EPA CDX

Registrants will be directed to DEQ's CROMERR registration web site, ERS, where they will supply valid e-mail addresses for both the submitter and company official, as well as other demographic information required by DEQ's Electronic Signature Agreement. For documents requiring electronic signature, the email address associated with the ESA will be used to provide notification of document submission and availability for review. In the event that a notification e- mail message is undeliverable, the email server will register this event. The ERS Administrator

will regularly check the ERS mailbox and respond to undelivered messages by attempting to obtain a valid email address by contacting the signatory or the company official authorizing the signatory over the phone. If the email address has changed since the certificate was issued, the submitter has to go through the process of registration. This procedure is also used when the submitter requests a change of email address.

Example 2 of Effective Approaches:

Example approach used by the Indiana IDEM eAuth system (this information was provided under Items 1 and 3 of the Indiana IDEM eAuth CROMERR Checklist, and not under Item 12):

SYSTEMS USING THIS APPROACH:

- Indiana IDEM eAuth

The applicant will complete portions of the signature agreement in an online eAuth Enabled Application (eA-EApp) registration form specifically tied to each eA-EApp. This form requires an email address entry, among other information. All user changes to an account profile for a facility immediately disable access to that facility. The eA-AppAdmin 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. The account owner must undergo another round of identity-proofing before the eA-AppAdmin will reactivate the account. A change to a 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), until the eA-AppAdmin completes the new identity-proofing and re-enables the user's account. At that time, the new email address becomes the email of record.

10. (Item 12: Automatic acknowledgment of submission) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(vi)

Common Issues / Deficiencies: No description of how system maintains records of the automated e-mail acknowledgements of submission to demonstrate that the notifications have been sent. The system needs to maintain a record of the automated e-mail acknowledgements of submission. Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Example 1 of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

SYSTEMS USING THIS APPROACH:

- OK DEQ EDRS

Edoctus captures and stores all emails (i.e., the date and time, address to which the email is sent, and the email contents). These emails are stored for the length of time required for retention of such records as set by the Oklahoma Department of Libraries, or the length of time required by rule, whichever is greater.

Example 2 of Effective Approaches:

Example approach used by the Indiana IDEM eAuth system:

All email notifications are logged in eAuth system components. At a minimum, the following information is logged:

1. eA-EApp system
2. Submission document type
3. User ID
4. Timestamp
5. Document ID
6. Sender email address
7. Recipient email address
8. Email body text content

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- Texas NetDMR
- Texas STEERS
- EPA NetDMR

11. (Item 15. Procedures to flag spurious credential use) (e-signature cases only) – 40 CFR § 3.2000(b)(5)(i)

Common Issues / Deficiencies: Incomplete description of processes for detecting and investigating signs of spurious credential use. Where applicants stated that they would review records or logs, missing detail often includes:

- what they would review
- how often
- what signs they would look for
- the procedures to be used if suspicious activity is identified

The system must provide a process for detecting spurious credential use. Note that this item must be addressed only for reports that require an electronic signature, including priority reports.

Example 1 of Effective Approaches:

Example approach used by the EPA CDX system:

SYSTEMS USING THIS APPROACH:

- EPA CDX

Three successive login failures will result in an account lock-out condition, which 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. For CDX PKI Enabled Applications, 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. 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.

Example 2 of Effective Approaches:

Example approach used by the EPA NetDMR system:

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA NetDMR

NetDMR includes functions that allow NetDMR Administrators to detect compromises. For example, each time a user logs in, the IP and date/time of the login is stored. Inconsistencies in the logins, such as different IP addresses, may indicate a compromised password. Additionally, NetDMR will only allow a user to maintain a single concurrent NetDMR session. If the user is already logged in, the previous login will be invalidated. Frequent, overlapping login attempts may indicate a compromised password. NetDMR will include fraud analysis functionality, in which the logs are periodically analyzed for irregularities. Irregularities will be flagged for NetDMR Administrators to investigate and take further action, if appropriate. The irregularities NetDMR will flag include inconsistencies in the logins, such as use of multiple IP addresses, frequent overlapping login attempts from different IP addresses, and irregular submission patterns (e.g., a user who has submitted a single DMR every month for the past 6 months, but then submits 50 in one month). If it is determined that a compromise has occurred, the affected account will be locked and the user will be contacted.

NetDMR also includes functions that allow NetDMR users to detect compromises. After each DMR is submitted, the submitter is sent a confirmation email. Also, after logging in, a list of the user's previous logins is displayed, including the date/time of the login and whether a submission was made during that session. If it is determined that a compromise has occurred, the user is required to lock their account and notify the Regulatory Authority.

12. (Item 19: Timely availability of copy of record (COR) as needed) – 40 CFR § 3.2000(b)(1)-(2)

Common Issues/Deficiencies: No description of how long it takes to retrieve a copy of record for program or enforcement staff. Some applications provided this information for the period when the COR was in short-term storage, but did not provide it for the period after it was moved to long-term storage.

Agency staff must be able to access CORs quickly enough to meet program and enforcement needs.

Examples of Effective Approaches:

Example approach used by the EPA NetDMR system:

NetDMR generates the COR during the submission process. The COR is available for review using NetDMR by registrants with the authority to view CORs for the specified permit. Internal staff are also able to view CORs. NetDMR will allow users to search for CORs on various data fields (e.g., Submitter, Permit ID, Date Range). Further, users will be able to view the COR online and download the COR for offline review. The CORs will be searchable and viewable using NetDMR for the entire length of time for which they are maintained in NetDMR (the retention schedule is described in the NetDMR application under CROMERR Checklist Item 20).

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR

13. (Item 20: Maintenance of copy of record (COR)) – 40 CFR § 3.2000(b)(1)-(2)

Common Issues / Deficiencies: No description of how the system prevents the alteration or deletion of CORs. Missing detail often includes:

- the electronic and physical security measures of the system to prevent unauthorized access to the system from outside, such as firewall, virus detection, intrusion detection, and access restrictions for the physical space where system components such as servers are housed
- safeguards against alterations of CORs by system administrators

The system must be able to prevent CORs from being altered or deleted by external intruders or by system administrators. In addition to describing such measures in the checklist, including attachments such as a security plan, description of safeguards, rules of behavior for system administrator, and other information can often help to satisfy the requirements of Item 20.

Example 1 of Effective Approaches:

Example approach to electronic measures to prevent unauthorized access used by the Texas STEERS system (this information was provided in supporting documentation for the Texas STEERS CROMERR checklist):

SYSTEMS USING A SIMILAR APPROACH:

- Indiana IDEM eAuth
- Texas STEERS

The WWW6 ColdFusion servers exist between two firewalls. This area is referred to as the 'DMZ.' The 'external' firewall intercepts all requests from the internet and redirects them to the appropriate server. The 'internal' firewall accepts requests through the default Oracle identification port (1521) from the ColdFusion IP addresses.

Example 2 of Effective Approaches:

Example approach to physical security from an attachment to the EPA NetDMR application:

Physical and environmental controls for the CDX Production environment are provided, reviewed, and maintained by the NCC located in RTP, NC in accordance with Agency Network Security Policy; OTOP 200.05; NCC Access Security Procedure; Computer Operations Security Data Center Sign-in Procedure; NCC Physical Security Plan; OARM/RTP Card Access Authorization and Usage Records; and the Draft EPA Qualitative Physical Security Risk Assessment for RTP Campus Draft March 2002. The controls include physical access authorization and control, monitoring physical access, visitor control, and access logs. For specific procedures see referenced documents.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Texas NetDMR
- Indiana IDEM eAuth
- EPA NetDMR
- North Dakota ERIS

Example 3 of Effective Approaches:

Example approach to safeguards against alterations by system administrators used by the EPA CDX system:

In order to prevent unauthorized access to the system or its data by operating personnel, CDX is operated according to the policies defined in the CDX Separation of Duties Guide. This document identifies the access controls, authorized actions, and minimal personnel security checks required for each defined operations role. All CDX personnel with access privileges to the production environment are required to have at least a Minimum Background Investigation (MBI) clearance check.

After a COR is created, CDX computes a SHA-1 hash value of all COR components. This hash value is then signed using a CDX server private certificate, and the signature value (and information regarding it) is saved within the database and written to the 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 provides an additional independent means of validating the integrity of COR content as maintained on the database servers. 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.

SYSTEMS USING A SIMILAR APPROACH:

- Delaware DNREC ORS
- Indiana IDEM eAuth
- North Dakota ERIS
- OK DEQ EDRS
- Texas NetDMR
- Texas STEERS
- EPA CDX
- EPA NetDMR
- EPA SDWIS

14. (Item 20: Maintenance of copy of record (COR)) – 40 CFR § 3.2000(b)(1)-(2)

Common Issues/Deficiencies: Incomplete description of how CORs were protected through file backups. Missing detail often includes:

- how frequently files are backed up
- what files are backed up
- whether backups are stored on-site or off-site
- provisions for disaster recovery

Systems must have procedures to back up COR files and ensure that backups are safely maintained and can restore CORs in case there is system disaster. In addition to describing such measures in the checklist, including attachments such as a backup plan, document retention schedule, disaster recovery plan, continuity of operations plan, and other information can often help to satisfy the requirements of Item 20.

Examples of Effective Approaches:

Example approach used by the OK DEQ EDRS system:

Submitted documents will be stored in human-readable format along with the digital signature(s) as copies of record in Edoctus. These documents will be protected from edits and preserved in exactly the form in which they were submitted. Read-only access to the documents will be available to authorized agency personnel and to the submitter for review. Documents will be preserved indefinitely in the document management system.

SYSTEMS USING A SIMILAR APPROACH:

- Indiana IDEM eAuth
- OK DEQ EDRS
- EPA CDX

All data at DEQ, including the data stored within Edoctus, are backed up on a nightly basis. These backups are also stored off-site, and DEQ will soon implement an advanced off-site SAN-to-SAN backup solution. DEQ is required to file an annual disaster recovery plan, which includes substantial provisions for recovery of data and resumption of operations in the event of a disaster.