UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

NOV 19 2007

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Determination that EPA's Proposed NetDMR System is Consistent with the Cross-Media Electronic Reporting Regulation (CROMERR) Standards

FROM: Molly A. O'Neill
Assistant Administrator and Chief Information Officer

TO: Catherine R. McCabe, Principal Deputy Assistant Administrator
Office of Enforcement and Compliance Assurance

This memorandum constitutes my determination that the Office of Enforcement and Compliance Assurance's (OECA) proposed NetDMR electronic reporting system, for the receipt of discharge monitoring reports under the National Pollutant Discharge Elimination System program (40 CFR 122.41 & 403.12), is consistent with the standards in CROMERR section 3.2000. I base my determination on the Agency-wide Technical Review Committee's (TRC) review of this system and the TRC's Recommended Basis of Decision. The approved OECA NetDMR CROMERR System Checklist, submitted by OECA on September 5, 2007, and the NetDMR CROMERR System Checklist Supporting Documentation, submitted by OECA on August 2, 2007, are attached.

In the October 13, 2005, notice of final rulemaking for CROMERR, the preamble states that "EPA's goal is that all its systems for receiving electronic reports be consistent with the CROMERR standards[.]" (70 Fed. Reg. 59848, 59860). In accordance with that goal, EPA established the TRC to, in part, review EPA systems for consistency with the CROMERR standards. OEI intends to include the NetDMR system in a Federal Register notice designating non-CDX data flows that have been certified for receipt of electronic reports.

States, tribes, and local governments choosing to use this system to receive electronic reports under their authorized programs must first apply to revise or amend those programs to include electronic reporting as required under 40 CFR Part 3. Each authorized program application must include the elements specified in §3.1000(b)(1) of the regulation, including a detailed description of how the system will satisfy each of the applicable requirements of CROMERR. Also, to the extent an authorized program's approach differs from the EPA system approach as approved, the authorized program application will need to document such differences for EPA consideration.

If you have any questions or comments, please direct them to Evi Huffer, OEI TRC Representative, at (202) 566-1697, huffer.evi@epa.gov or David Schwarz, OEI TRC Representative, at (202) 566-1704, schwarz.david@epa.gov.

Attachments

cc: Mark Luttner
Michael Stahl
Lisa Lund
David Hindin
Tom Seaton
Michael Ledesma
Michael Barrette
Evi Huffer

USEPA OECA NetDMR
CROMERR System Checklist Supporting Documentation

Last updated: August 2, 2007

Item 1b-alt
For EPA Regions with primacy for administering the NPDES program, a paper copy of the signed permit, subscriber agreement and any delegation of authority as required by 40 CFR 122.22 will be maintained in the Regional file room according to the retention schedule specified in EPA Records Schedule 419, using the NARA disposal authority N1-412-97-1/1. This authority specifies records be held in the Regional office for 5 years, upon which time they may be sent to the Federal Records Center. Access to the Regional file room is restricted to personnel authorized by the Regional Records Management Officer.

Item 2
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. 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.

Item 3
NetDMR will require all users to change their password at minimum of every 90 days.

NetDMR will require all users to provide the answer to 5 secret questions.

Item 16
An investigation will begin within one business day of when an account is suspected of being compromised. The investigation will determine whether a compromise has occurred. If it is determined that the account has been compromised, the account will be immediately locked.

Item 20
The NetDMR application will be hosted at EPA in the CDX environment. The following reflect the procedures in place for this environment.

CORS
The COR will be maintained for at least 6 years from the date of submittal.

Database Backups
NetDMR will be deployed in the CDX environment. CDX servers are backed up using NCC's standard 90-day VERITAS tape backup procedure.

Physical Security
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.

EPA OECA NetDMR - CROMERR System Checklist – Version 2.0
September 5, 2007

Item	GENERAL NOTE: State implementations of this system will require review and approval by EPA. To the extent that a State has adopted the system as described in this application, EPA review of that system will be largely a formality. Where a State chooses to deviate from the system as described in this application, those deviations will be the subject of more thoroughgoing review and analysis by EPA.
	Registration (e-signature cases only)
	1. Identity-proofing of registrant
	Business Practices: NetDMR will use a Subscriber Agreement. Per CROMERR 3.2000(b)(5)(vii)(C), the receipt of a signed Subscriber Agreement is sufficient proof of the user's identity. See Item 1b-alt for more information on the Subscriber Agreement. The Regulatory Authority will review the information provided and perform additional identity proofing to the best of their ability.
	System Functions: See Item 1b-alt for more information on the information contained in the Subscriber Agreement and how the user would provide this information.
	Supporting Documentation (list attachments): (placeholder for additional regulatory specific identify proofing processes)
	1a. (priority reports only) Identity-proofing *before* accepting e-signatures
	Business Practices: See Item 1 for how identity proofing will be performed using a Subscriber Agreement. See Item 1b-alt for more information on the information contained in the Subscriber Agreement, how the user will provide the information, and the verification business processes used by the Regulatory Authority to assure the requested access is appropriate for the user.
	System Functions: NetDMR will not allow a user's electronic signature device to sign electronic documents until the Subscriber Agreement has been received and verified by the appropriate regulating authority. See Item 1b-alt for more information on the information contained in the Subscriber Agreement and how the user would provide the information.
	Supporting Documentation (list attachments):
	1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)
	1bi. (priority reports only) Verification by attestation of disinterested individuals
	Business Practices: N/A – use 1b-alt Subscriber Agreement alternative
	System Functions: N/A – use 1b-alt Subscriber Agreement alternative

	Supporting Documentation (list attachments): N/A – use 1b-alt Subscriber Agreement alternative

1bii. (priority reports only) Information or objects of independent origin	
	Business Practices: N/A – use 1b-alt Subscriber Agreement alternative
	System Functions: N/A – use 1b-alt Subscriber Agreement alternative
	Supporting Documentation (list attachments): N/A – use 1b-alt Subscriber Agreement alternative
1b-alt. (priority reports only) Subscriber Agreement alternative	
	Business Practices: Per CROMERR requirements, Subscriber Agreements will be stored for at least 5 years after the associated electronic signature device has been deactivated. See Item 1 and 1a for how the Subscriber Agreement meets the identity proofing requirements. See Item 2 for how the Subscriber Agreement is used by the Regulatory Authority to determine the requestor's signing authority. See Supporting documentation for business processes for storing the Subscriber Agreement.
	System Functions: Per the definitions in CROMERR, a Subscriber Agreement is "an electronic signature agreement signed by an individual with a handwritten signature". The user will complete portions of the Subscriber Agreement in an online NetDMR form. The user will then print, sign, and mail the subscriber form to the appropriate Regulatory Authority. The user's electronic signature device will not be able to sign electronic documents until the Subscriber Agreement has been received by the appropriate Regulatory Authority and the authority has verified the information (see Business Practices). The online NetDMR form requires the requestor to enter the following data: 1. Full name. 2. Email address. The user will be required to enter their email address two separate times to assure it was entered correctly. 3. The permits for which the user is requesting signing privileges. 4. For each permit, whether the user has direct authority under the rules to sign the eDMRs for the facility or the authority is being delegated to him/her. 5. If the authority is delegated, the name and title of the person delegating the authority. The agreement includes language, in the first person, stating that the requestor: 1. Agrees to a. Protect their account password from compromise, not allow anyone else to use the account, and not share the password with any other person. b. Promptly report to the Regulatory Authority any evidence of the loss, theft, or other compromise of the user account password. c. Notify regulating authority if the user ceases to represent any of the requested facilities as the submitter for the organization's electronic reports to NetDMR as soon as this change in

relationship occurs.
   d. Review, in a timely manner, the acknowledgements (email and onscreen) and copies of submitted documents using their account.
   e. Report any evidence of discrepancy between the document submitted, and what NetDMR received.
2. Understands that he/she will be held as legally bound, obligated, and responsible by the electronic signature created as by a handwritten signature.

NetDMR will automatically validate that the requested permits are valid for electronic reporting and determine to which Regulatory Authority the signed Subscriber Agreement should be mailed. The user will then print, sign, and mail the agreement to the specified authority. If the authority is being delegated to the requestor, the delegating authority must also sign the Subscriber Agreement.

See Item 3 for information on how the user account is created.

Supporting Documentation (list attachments):
See attachment CROMERR_checklist_NetDMR_Supporting_v2.0.doc.
(attach sample Subscriber Agreement)

2. Determination of registrant's signing authority

Business Practices:
Regulatory authorities must receive a signed Subscriber Agreement from each user that is requesting the ability to sign DMRs. Regulatory authorities will, to the best of their 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. Once verification is complete, the Regulatory Authority will assign the user's account the appropriate NetDMR signatory permission. See Supporting Documentation for more information on the specific verification processes that will be used.

System Functions:
For information on the Subscriber Agreement, see Item 1b-alt.

Supporting Documentation (list attachments):
See attachment CROMERR_checklist_NetDMR_Supporting_v2.0.doc.

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

Business Practices:
See Item 1b-alt for the business processes used to process received Subscriber Agreements. See supporting documentation for additional business processes relating to this item.

System Functions:
I. NetDMR provides the following mechanisms to securely issue signing credentials:
1. The Subscriber Agreement contains language requiring the user to protect their signing credential, not share it with anyone else, and report any compromise to the Regulatory Authority (see Item 4 for more information on the contents of the signature agreement).
2. The account creation process provides numerous levels of verification. The attached RegistrationFlow document provides the overall flow for creating a new NetDMR account and gaining signatory privileges. Specific notes on the account creation process described in the diagram:
   a. The Verification Key will be automatically generated by NetDMR through the use of an algorithm that generates a random, globally unique key. For example, the SecureRandom[1] java class specification will be used to generate the random portion of the key and the system

time, IP, and username will provide the unique portion of the key. This information would then be hashed using a one way algorithm (SHA-256[2]) to generate the actual key. The Verification Key will only be valid for only 60 days, after which the user will have to re-start the registration process.

b. The registrant will be emailed a URL to verify their email address. The URL included in this email will link to a secure verification page (Secure Sockets Layer protocol v3 or Transport Layer Security v1.0). It will include the Verification Key as a query string parameter to allow NetDMR to verify the validity of the key and immediately challenge the user with one of the security questions answered by the registrant during the registration process.
c. After the registrant submits their information and NetDMR emails the specified account, the user will be presented with a notification page indicating that he/she should receive the email within the next 24 hours, and that the registrant should contact the appropriate Regulatory Authority if he/she does not receive the email.
d. The security question serves to link the original registrant with the user accessing the verification page and assure that the registrant has access to the specified email account. If an invalid account was specified, the original registrant would never receive the Verification Key and would not be able to verify the account. If the wrong person received the email, he/she would not know the answer to the secret question to verify the account.
e. If the registrant enters the wrong answer to the security question 3 times, the verification process is locked, an email is sent to the registrant, and the user must contact the Regulatory Authority to continue (or create a new account).
f. The registrant must set a password during the verification process. The password must be between 8 and 20 characters and contain letters and numbers. The first character must not be a number. Once the password is changed the Verification Key is no longer valid.
g. Only verified accounts have access to NetDMR beyond the verification page. Verified accounts have limited access to NetDMR until a Regulatory Authority grants the account signatory rights to a permit.
h. The registrant's password and responses to the security questions are stored in the database in a hashed format using a secure hash algorithm (SHA-256[2]). One-way hashes are designed to prevent the retrieval of the pre-hashed data (or something else that hashes to the given hash) given just the hash. This significantly reduces the possibility of learning the password or security question responses by gaining access to the database.
i. A unique 8 character random password salt[2] is created using the SecureRandom[1] java class for each user and stored in the NetDMR database. While the likelihood of SecureRandom generating the same random salt for multiple users is remote, NetDMR will verify the generated salt is unique within the database prior to assigning it to the user. A salt is a set of characters that is appended to the user's password prior to creating the hashed value of the password. For more information on salts see http://msdn.microsoft.com/msdnmag/issues/03/08/SecurityBriefs/. The use of a salt primarily strengthens the protection of passwords as follows:
    1. The addition of the user specific salt to each user's password assures the salt+password combination for each user is unique. A one-way hashing algorithm is designed to assure that the hashed forms of any two distinct values do not hash to the same value (defined as a collision). While such collisions do occur, the likelihood of such collisions is remote. The use of a salt makes it extremely unlikely that two users who have the same password will have the same hashed password.
    2. Makes it extremely difficult to use a pre-generated list of hashed common passwords to determine a user's password. A malicious user would need to know the user's salt value to create a pre-generated list of hashed passwords for each user.

3. The request for signatory rights provides numerous levels of verification. The attached RegistrationFlow document contains the overall flow for creating a new NetDMR account and gaining signatory privileges. Specific notes on the process for requesting and receiving signatory rights:
    a. Only verified accounts can request or be granted signatory access to a permit.
    b. If a malicious user intercepts the verification email, knows the answer to the secret question, and is able to access NetDMR prior to the intended registrant he/she would still need to

complete, print, sign, and mail the Subscriber Agreement to the Regulatory Authority before he/she would be able to submit a fraudulent eDMR. This would require the malicious user to know the applicable permit IDs for the user, and submit a forged Subscriber Agreement.

c. If a malicious user performed the steps in (b), the intended recipient would be able to detect the compromise. Since users are required to set a new password when using a Verification Key, the intended registrant would receive an email notification of a password change that he/she did not make. Also, when the intended registrant attempts to use the provided Verification Key he/she would be notified that the key had already been used.
d. The verification business process used by the Regulatory Authority will be regulatory-authority specific. For more information on the verification business process, see Item 1b-alt.

II. NetDMR provides additional credential protection throughout the lifetime of the account:

1. NetDMR requires all users to provide the answer to five security questions at the time a user registers to use the system. The list of available questions will be provided by NetDMR. The questions will be chosen such that the expected answers should be common knowledge to the user, but should not otherwise be readily available (e.g., found on Google). For example, questions could include: "The make and model of the first car I owned" or "The name of my first pet". A list of at least ten questions will be provided to the user. The questions and answers are stored within the NetDMR database. The questions will be stored in plaintext. The answers will be hashed using the SHA-256 algorithm. Wherever the user is required to provide the answer to a security question, NetDMR will randomly (via SecureRandom[1] java class specification) choose one of the security questions on file for the user. The answer provided by the user will be hashed and compared to that stored in the database.
2. Users can change their password, security questions, and security question answers at any time through NetDMR. Users must reenter the account's password and answer the security question prior to changing any account information.
3. NetDMR requires users to change their password after a specified time period to something that has not been one of the account's past 10 passwords. The exact time period is specified by the appropriate business policy.
4. An Account is locked after three unsuccessful login attempts, three unsuccessful attempts to sign a DMR, or three unsuccessful attempts to change account information within a 24 hour period. Once locked:
   i. The account can not be used to log in to NetDMR.
   ii. An email is sent to the user to notify them that the account was locked. If the account was locked due to unsuccessful login attempts, as opposed to the Regulatory Authority locking the account due to suspected compromise, the user can have the account unlocked by either providing the answer to a security question or contacting the Regulatory Authority. If the account was locked for any reason other than exceeding the number of unsuccessful login attempts, the user must contact the Regulatory Authority to have the account unlocked.
   iii. An email is sent to the Regulatory Authority describing the potential problem.
5. When a locked account is unlocked, the process outlined in I.2 will be performed to change the password. A new Verification Key will be generated and emailed to the user. The user will not be able to log into NetDMR until he/she visits the verification page and reset the account password.

Supporting Documentation (list attachments):
See RegistrationFlow_v2.0.jpg
See attachment CROMERR_checklist_NetDMR_Supporting_v2.0.doc.

4. Electronic signature agreement

Business Practices:
See Item 1b-alt

	System Functions: NetDMR will use a Subscriber Agreement, which is defined as "an electronic signature agreement signed by an individual with a handwritten signature". The content of the Subscriber Agreement is described in Item 1b-alt.
	Supporting Documentation (list attachments):

Signature Process (e-signature cases only)	
5. Binding of signatures to document content	
	Business Practices:
	System Functions: **Signature Process** The signature process is a multi-step process. The attached SignatureFlow diagram illustrates the overall flow. NetDMR allows users to submit multiple eDMRs within a single transaction. However, NetDMR will create a unique Copy of Record (COR) for each eDMR that is submitted. NetDMR also allows users to upload supporting documentation (i.e., attached files) that should be associated with the eDMR. The process used to create the COR and additional information on the process described in the diagram, and handling of attachments, are detailed below. Data Document • The data document is created for each submitted eDMR. The data document is an XML document where the XML tags provide semantic meaning to the data. The document includes, at a minimum: 1. All the user-provided data for the eDMR. 2. Legal Certification Statement to be displayed to user during signing process (see Item 7). 3. Hashes of each attached file 4. Metadata about each attached file (e.g., name, type, etc) Signing the Document • Users must indicate which of the DMRs displayed on the Verification page he/she intends to sign (e.g., through a checkbox next to each DMR). • NetDMR will randomly choose one of the secret questions on file for the user's account. The user must enter the account's password and provide the answer to the question in order to sign the DMR(s). • If the user enters the wrong password or answer to the secret question 5 times within a 24 hour period, the account will be locked and can not be used until it is unlocked. See Item 3 for more information on how the account can be unlocked. Hash Algorithm • NetDMR uses SHA-256 to generate all hash values. This is the current approved FIPS standard[2]. Confirmation Number • A unique confirmation number is generated based on the user account information, IP of user, and current system date. The confirmation number is unique to the submission. If multiple eDMRs are submitted by the user at the same time, each eDMR within the submission will have the same confirmation number. Submission Receipt • A submission receipt is created for each eDMR that is submitted. The submission receipt is an XML

document where the XML tags provide semantic meaning to the data. The receipt includes

1. Confirmation Number
2. The hash of the data document
3. Date/Time of the submission
4. Identifying information from the signing account, including:
    a. The user's full name
    b. Account Login
    c. Email Address
    d. Hashed Password (at time of signing)
5. IP of submitting computer.

Copy of Record (COR)

- The COR is a zip file created for each submitted eDMR. It contains
    1. Data document
    2. XSL stylesheet (to apply against Data XML document)
    3. Attached files (if applicable)
    4. Submission receipt

COR Signature

- Each NetDMR installation will have an RSA 1024 bit asymmetric key that will only be used for digital signatures (e.g., not used to establish SSL connections). The existing EPA certificate generation infrastructure for the Exchange Network will be analyzed for possible reuse to generate the NetDMR digital signature keys.

- NetDMR will use its private key to digitally sign[4,5] the CORs. The signature will be executed against a message digest created from the COR using the SHA-256[2] hashing algorithm.

Confirmation Page/Email Acknowledgement

- The confirmation page and email acknowledgement will include:
    1. The confirmation number of the submission.
    2. The COR signature.
    3. The public NetDMR RSA key.
    4. Instructions to download the COR.
    5. Instructions to view the COR online.

COR Alteration Protection

The purpose of the NetDMR digital signature is to provide assurances that the COR was submitted through NetDMR. Digital signatures can be verified by generating the hash value of the COR and comparing it to the hash retrieved by applying the NetDMR public key to the digital signature. The three primary COR alteration use cases the signature process is designed to protect against are detailed below, along with the processes NetDMR will use to mitigate the risk.

Use Case A. Signatory Falsification

Description: A signatory claims that NetDMR does not contain the actual submitted data by providing an alternate COR and digital signature. The steps to replicate this use case include:

1. The signatory submits a document to NetDMR and receives a copy of the COR.
2. The signatory alters the COR and recalculates the hash value.
3. The signatory claims the COR in NetDMR does not represent that actual submitted data and provides the modified COR and hash value as proof.

Mitigation: This use case is mitigated as follows:

- It is computationally infeasible for the user to forge the digital signature without the private key.
- The NetDMR private key will be protected from unauthorized access by storing it in a secure location on the NetDMR server. Physical access to the server will be restricted as specified in Item 20.
- A NetDMR administrator is required to specify which key pair on the server NetDMR will use for digital

signatures. NetDMR will log any changes made to the key/pair used by NetDMR for signing CORs.

These strategies protect NetDMR from unauthorized users attempting to swap a secure key pair with a compromised one. Such a change would require access to both the physical server and either the database or Administrator access rights to the NetDMR.

Use Case B. Regulatory Authority Staff Falsification
Description: A Regulatory Authority staff member alters the COR in NetDMR without the signatory's knowledge. A possible scenario includes an attempt to alter a Signatory's submission from being compliant to non-compliant.

Mitigation: This use case is mitigated through the following measures:

- Alterations would require access to the NetDMR database. The staff member would also need a detailed understanding of the data model to make all the necessary alterations to the COR, regenerate the hashes, and modify the various logs.
- The staff member would require access to the NetDMR private key in order to generate a new signature. The key pair can only be registered for use with NetDMR through direct access to the NetDMR server. Physical access to the server will be restricted as specified in Item 20. Additionally, a NetDMR Administrator must configure NetDMR to use the registered key pair.
- NetDMR allows Administrators to specify one or more email addresses that are copied on all submission acknowledgement emails. The submission acknowledgement email contains the signature of the COR. The staff member would have to alter the signature contained in the original email sent to these addresses to avoid detection of the change.
- The NetDMR database will be periodically backed up. The staff member would need to alter the backups to reflect the changed data. The backup process is described in Item 20.
- If the internal user was able to circumvent the numerous protections, the signatory would still have a valid COR signature. As described in Case A, it is computationally infeasible for the Signatory to create a valid NetDMR signature without the private key. The fact that the Signatory has a valid signature would provide strong evidence that the data in NetDMR had been altered.

To alter the submission without detection the staff member (or members) would require access to the database, the NetDMR server, tape backups, and the email system. The staff member would also need enough detailed knowledge of NetDMR to make all the necessary modifications within the database. It is extremely unlikely a single staff member, or even a couple staff members, would have the access and knowledge required to make all necessary changes to prevent detection. Additionally, the dual protection in place for registering and configuring the NetDMR public/private key makes it difficult for a single user to substitute a new key pair.

Use Case C. Third Party Modification
Description: A third party alters the COR in NetDMR without the knowledge of the Regulatory Authority or signatory. A possible scenario includes a group attempting to alter a submission from being compliant to non-compliant in an attempt to cause enforcement actions against a facility.

Mitigation: Without the cooperation of the signatory or an internal staff member, all mitigation strategies applied to Case A and Case B would apply to this use case. In addition, the malicious user would need to gain access to the network on which NetDMR is installed.

Supporting Documentation (list attachments):
See SignatureFlow_v2.0.jpg

6. Opportunity to review document content

Business Practices:

System Functions:
During the signing and submission process (See Item 5), the user will be presented with a verification page. The verification page includes:

1. A read-only view of the DMRs the user selected. The data will be displayed in a manner that provides the user the opportunity to review the data, but does not require the user to review it. For example, the DMR may be displayed in a summary format with the ability for the user to expand the eDMR to display all the information.
2. Links to download and view any documents that were attached to the eDMR.
3. Checkboxes to confirm selection of the DMRs to be signed and submitted.
4. Certification statements (see Item 7).
5. A text box for supplying the account password.
6. A randomly selected security question on file with the user's account and a text box to supply an answer.

Supporting Documentation (list attachments):

7. Opportunity to review certification statements and warnings

Business Practices:

System Functions:
During the signing and submission process (See Item 5), the user will be presented with a verification page. The verification page includes:

1. Information in Item 6.
2. A certification statement (in the first person) stating the user:
    a. Is the owner of the account he/she is using.
    b. Has protected the account and password and is in compliance with the Subscriber Agreement.
    c. Has the authority to submit the data on behalf of the facility.
    d. Agrees that providing the account password to sign the document constitutes an electronic signature equivalent to his/her written signature.
    e. Understands this attestation of fact pertains to the implementation, oversight, and enforcement of a federal environmental program and must be true to the best of the user's knowledge
    f. Current password is not compromised now or at any time prior to the submission
3. A certification statement appropriate to the Regulatory Authority.

Example language, provided by Michael Ledesma (EPA/OECA) that would appear to meet most of 2a,2b,2e,and 2f:

I certify that I have not violated any term in my Electronic Signature Agreement and that I am otherwise without any reason to believe that the confidentiality of my Personal Identification Number (PIN) and/or password have been compromised now or at any time prior to this submission. I understand that this attestation of fact pertains to the implementation, oversight, and enforcement of a federal environmental program and must be true to the best of my knowledge.

Supporting Documentation (list attachments):

EPA OECA NetDMR - CROMERR System Checklist – Version 2.0
September 5, 2007

Submission Process

8. Transmission error checking and documentation

Business Practices:

System Functions:
See Item 5 for the submission process and more detail on how the submission process protects against alterations once it has been received by NetDMR.

The integrity of the submission is protected in the following ways:

1. No alteration of the document content is expected during transmission or after it is received.
2. The entire session takes place over the Secure Sockets Layer (SSL) protocol v3 or Transport Layer Security v1.0. This protects against man-in-the-middle attacks.
3. The information in the data XML document used for the verification page (see Item 5) comes from data already stored in the NetDMR database. No updates to this data are performed at any time during or after the submission process. With the protection in place from man-in-the-middle attacks, this provides a high level of assurance that the user is seeing the data as it is stored in the database.
4. The data XML document and all attached files are included, without alteration, in the COR. This assures that the COR contains the same data, in the same format, as what the user was given the opportunity to review (see Item 6).
5. The COR signature (see Item 5) is provided to the user in an email acknowledgement along with instructions to access the COR. The email allows the user to detect modifications to the submission. See Item 5 for more information.
6. It is computationally infeasible for the user to create a valid COR signature without the NetDMR private key. This protects against users modifying the COR and attempting to claim the data were altered in NetDMR (see Use Case A in Item 5)
7. The validity of the signed COR can be determined using the NetDMR public key. This assures that the NetDMR private key was used to sign the COR.
8. The data hash and COR signature can be recomputed, if needed, to compare against the original values.
9. The submitter has the opportunity to review the data during data entry, the submission process, and the COR review process.

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:

System Functions:
Submitters are informed and made aware of the availability of CORs in multiple ways:

1. The submitter is automatically sent an email notification after each submission. The email contains information on how to access the COR.
2. Submitters have the ability to view CORs at any time using NetDMR. This will be documented in the NetDMR help system and manual.

3. After each login, the user is presented with a list of the past 10 login sessions including the date/time and whether any DMRs were submitted during the session. If submissions were made, a link to view the CORs of the submissions will be included.

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:

System Functions:
See Item 5 for information on what is contained within the COR. The COR is a zip file which contains all the appropriate information for the submission. The documents within the COR are of two types:

XML Documents
The XML tags used in these documents relate the user-supplied data to the context in which the data were provided. Item 5 for more information on the contents of the XML documents.

Attached Files
Users can attach supporting documents to the submission. These documents are stored in their native format. For example, a Microsoft Word document will be stored in the COR file as a Microsoft Word document. The user is required to have the appropriate application to view the attached file. For example, users must have Microsoft Word or a program that can understand the Word format in order to view the Word document.

See Item 9c for how users can view the COR.

Supporting Documentation (list attachments):

9c. Providing the copy of record

Business Practices:

System Functions:
NetDMR creates the COR, a zip file, during the submission process. See Item 5 for more information on the process for creating the COR and the contents of the COR. Signatories are notified of the COR in an email acknowledgement and on the confirmation page during the submission process. The email includes instructions for viewing the COR. The confirmation page contains both a link to download the COR as well as a link to view the COR online. All users with appropriate access for a particular permit can view the CORs for that permit. They can view submitted CORs by logging into NetDMR and searching for CORs for the specified permit.

The COR can be presented in a human-readable format in two ways:

1. Download
   NetDMR allows users to download the COR. After unzipping the COR, the user can apply the XSL stylesheet to the Data XML document to present it in a friendlier html format and view all the supporting

documents that were attached to the eDMR submission.

2. Online Viewing
NetDMR would provide a mechanism to allow user to view the contents of the COR online. NetDMR would automatically unzip the submission zip file to retrieve the files. The user can view the Data XML document, with the XSL stylesheet applied, and download any supporting documents that were attached to the eDMR submission. The user is required to have the appropriate application installed to view the attached file. For example, users must have Microsoft Word or a program that can understand the Word format in order to view the Word document.

Supporting Documentation (list attachments):

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

Business Practices:
The anticipated reasons a user would want to repudiate a COR include:
1. The data submitted is incorrect, and a correction needs to be provided.
2. The user did not submit the COR.

NetDMR allows users to submit corrections to a DMR previously submitted through NetDMR. Users can also replace attachments that were previously submitted. Therefore, users should not repudiate a NetDMR submission due to incorrect data. Instead, he/she should submit a corrected eDMR, which would generate a new COR. In this manner, the entire history of the DMR, including all corrections, will be documented.

If the user did not submit the COR, the user's signature device has been compromised. The user is required to immediately lock his account to prevent additional compromises and contact the Regulatory Authority. After calling the Regulatory Authority, the extent of the compromise will be assessed to determine whether any additional submissions need to be repudiated. The signatory and Regulatory Authority will also investigate how the account may have become compromised in order to prevent future occurrences. The Regulatory Authority will flag each fraudulently submitted COR as repudiated.

System Functions:
The help system will document the repudiation process.

The system allows Regulatory Authorities to flag CORs as repudiated.

Supporting Documentation (list attachments):

11. Procedures to flag accidental submissions

Business Practices:
If a user determines that he/she accidentally submitted a DMR, the submission can be corrected with a follow-up submission, or repudiated. The preferred approach would be for the user to submit a correction. If the user would rather repudiate the submission, the user must contact the appropriate Regulatory Authority. See Item 10 for the repudiation process and system functions.

System Functions:
NetDMR provides multiple mechanisms to prevent accidental submissions:
1. NetDMR performs a QA analysis on each DMR to validate that all required data points are provided. Only DMRs that pass the QA analysis can be submitted.
2. The NetDMR submission process uses a multi-step approach to reduce the likelihood of accidental submissions.
    a. Users must select the DMR(s) they intend to submit.
    b. Users are given the opportunity to review the selected data in a read-only manner.

c. Users must confirm their intent to submit by providing their password and security question answer on the verification page.

3. While it is unlikely that a user will proceed through the submission steps accidentally, in such a case, there are additional mechanisms in place to assist the user in identifying and correcting an accidental DMR submission:
   a. Submitters are sent an email after every submission.
   b. A list of previous logins is displayed every time a user logs in. The login list indicates whether or not a submission was made during that session.
   c. Users can review the CORs of all previous submissions using NetDMR.

NetDMR maintains all CORs for the retention period specified in Item 20.

Supporting Documentation (list attachments):

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

Business Practices:

System Functions:
NetDMR sends an acknowledgement email to the email address on file for the submitter after every submission. An email log is kept to track that the acknowledgement was sent.

Supporting Documentation (list attachments):

Signature Validation (e-signature cases only)

13. Credential validation (See 13a through 13c)

13a. Determination that credential is authentic

Business Practices:

System Functions:
NetDMR will compare the hashed form of the user-supplied password (appended with the user salt) and the hashed form of the answer to the secret question provided during the signing process to the hashed form of the user's password and the hashed form of the user's response to the secret question stored in the database. See Item 3 for more information on the user password salt.

Supporting Documentation (list attachments):

13b. Determination of credential ownership

Business Practices:

System Functions:
NetDMR will compare the hashed form of the user-supplied password (appended with the user salt) and the hashed form of the answer to the secret question provided during the signing process to the hashed form of the user's password and the hashed form of the answer to the secret question stored in the database. See Item 3 for more information on the user password salt.

Supporting Documentation (list attachments):

13c. Determination that credential is not compromised

Business Practices:
Administrators will periodically review the results of the fraud analysis and the login logs to determine if an account has been compromised. If it is determined that a compromise has occurred, the affected account will be locked, preventing the user from signing eDMRs, and the user will be contacted to address the situation.

System Functions:
NetDMR includes functions that allow NetDMR Administrators and users to detect credential compromises. See Item 15 for a description of these functions. NetDMR allows a user to lock his/her account if he/she suspects the account has been compromised. Administrators also have the ability to lock any user's account. The fact that the account was not locked at the time the eDMR was signed provides evidence that neither the user nor administrators believed the credential was compromised at that time.

See Item 3 for a description of how the account is protected from compromise.

Supporting Documentation (list attachments):

14. Signatory authorization

Business Practices:
See Item #2 for the process NetDMR Administrators use to grant signatory authority to NetDMR users.

System Functions:
The NetDMR authorization system includes a "submit" role that grants permission for a user to sign a DMR. This role is associated with a user and each permit for which he/she has signatory authority. NetDMR uses the authorization system to determine whether a given user is authorized to submit a given DMR.

Supporting Documentation (list attachments):

15. Procedures to flag spurious credential use

Business Practices:
Administrators will periodically review the results of the fraud analysis and the login logs to determine if an account has been compromised. If it is determined that a compromise has occurred, the affected account will be locked, preventing the user from signing eDMRs, and the user will be contacted to address the situation.

System Functions:
NetDMR includes functions that allow NetDMR Administrators to detect the possibility that a user's device has been compromised:

1. Each time a user logs in to NetDMR, the IP and date/time of the login is stored. Inconsistencies in the logins, such as different IP addresses may indicate a compromised password.
2. 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. If overlapping login attempts are frequently made, it may indicate a compromised password.
3. 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 are:
    a. Inconsistencies in the logins, such as use of multiple IP addresses.
    b. Frequent overlapping login attempts from different IP addresses.
    c. Irregular submission patterns. An example of an irregular pattern would be a user who has submitted a single DMR every month for the past 6 months, but then submits 50 in one month.

NetDMR includes functions that allow NetDMR users to detect the possibility that their account has been compromised.

1. After each DMR is submitted the submitter is sent an email acknowledging the submission.
2. After logging in to NetDMR, a list of the user's previous logins is displayed, including the date/time of the login and whether or not 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.

Supporting Documentation (list attachments):

16. Procedures to revoke/reject compromised credentials

Business Practices:
See attachment CROMERR_checklist_NetDMR_Supporting_v2.0.doc for the guideline regarding the timeliness of administrator action when account compromise suspected.

System Functions:
Users are able to lock their account and NetDMR administrators are able to lock any user's account. A user or administrator will lock the user account if evidence suggests the account has been compromised. A locked account can not be used to sign an eDMR or log in to NetDMR.

Supporting Documentation (list attachments):

17. Confirmation of signature binding to document content
Business Practices:
System Functions: NetDMR submitters will not use digital signatures to sign electronic documents. Instead, submitters will use a password. The submission process is provided in Item 5. As described in the process, identifying account information from the submitter's account will be inserted into the COR of the submission to bind the submitter's signature to the document content. The signature binding will be confirmed and the document integrity verified by recalculating the signature of the COR and comparing it to the signature generated at the time of submission. If any part of the COR was altered, including the signature binding information, the new signature would differ from the original.
Supporting Documentation (list attachments):

Copy of Record
18. Creation of copy of record (See 18a through 18e)
18a. True and correct copy of document received
Business Practices:
System Functions: See Item 5 for the contents of the COR and the process used to assure it is a true and correct copy of the data.
Supporting Documentation (list attachments):
18b. Inclusion of electronic signatures
Business Practices:
System Functions: See Item 5 for the contents of the COR and information on how the electronic signature is included in the document.

Supporting Documentation (list attachments):

18c. Inclusion of date and time of receipt

Business Practices:

System Functions:
NetDMR includes the date and time of the submission in the COR. See Item 5 for more information on the contents of the COR.

Supporting Documentation (list attachments):

18d. Inclusion of other information necessary to record meaning of document

Business Practices:

System Functions:
The COR is a zip file which contains all the appropriate information for the submission. See Item 5 for more information on what the COR contains. The documents within the COR are of two types:

XML Documents
The XML tags used in these documents relate the user-supplied data to the context in which the data were provided. Item 5 for more information on the contents of the XML documents.

Attached Files
Users can attach supporting documents to the submission. These documents are stored in their native format. For example, a Microsoft Word document will be stored in the COR file as a word document. It is assumed that the supporting documents are, by themselves, sufficient to understand the meaning of the documents.

Supporting Documentation (list attachments):

18e. Ability to be viewed in human-readable format

Business Practices:

System Functions:
See Item 9b and 9c for more information on how the COR is provided in a human-readable format.

Supporting Documentation (list attachments):

19. Timely availability of copy of record as needed

Business Practices:

System Functions:
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 at least the following fields:

1. Submitter.
2. Permit ID.
3. Date Range.

Users will be able to view the COR online and download the COR for offline review (see Item 9c). The CORs will be searchable and viewable using NetDMR for the entire length of time for which they are maintained in NetDMR. See Item 20 for the retention schedule.

Supporting Documentation (list attachments):

20. Maintenance of copy of record

Business Practices:

System Functions:
CORs
NetDMR CORs are stored/retained in the NetDMR database, which resides on a database server. Submissions are stored in the database as a BLOB. A BLOB is a large block of data stored in a database and is a Binary Large Object. A BLOB has no structure that can be interpreted by the database management system, but is known only by its size and location. The use of BLOB is standard with database products when dealing with large data sizes. A document ID is associated with each COR BLOB. Each unique document ID is associated with a specific confirmation number. Each unique confirmation number is associated with a specific submission through NetDMR. The CORs can be searched, viewed, and downloaded as specified in Item 19. NetDMR will maintain CORs per the retention policy of the NPDES regulations and the Regulatory Authority. See the supporting documentation for the exact length of time CORs will be stored.

Logs
The NetDMR COR, described in Item 5, contains the data submitted, date/time of the submission, the user who made the submission, and additional information necessary to establish what was submitted and who submitted it. In addition to the COR, NetDMR maintains various logs (e.g., email and login) that could provide supplemental information to that stored in the COR. These logs will be kept for 6 years, after which they will be deleted.

Database Backups
See the supporting documentation for the more information on the frequency of database backups.

Physical Security

	See the supporting documentation for the more information on the physical security.
	Supporting Documentation (list attachments): See attachment CROMERR_checklist_NetDMR_Supporting_v2.0.doc.

References:
[1] SecureRandom Specification: http://java.sun.com/j2se/1.4.2/docs/api/java/security/SecureRandom.html
[2] NIST Hash Function Policy:
http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NIST_Policy_on_HashFunctions.htm
[3] Salt Description: http://msdn.microsoft.com/msdnmag/issues/03/08/SecurityBriefs/
[4]Federal Information Processing Standards (FIPS)-approved algorithms for generating Message Digest:
http://www.csrc.nist.gov/CryptoToolkit/tkhash.html
[5]FIPS-approved algorithms for generating/verifying digital signatures:
http://www.csrc.nist.gov/CryptoToolkit/tkdigsigs.html