CROMERR System Checklist	
Item	**Delaware Department of Natural Resources and Environmental (DNREC) Online Reporting System Compliant with CROMERR (DNREC ORS)**
Registration (e-signature cases only)	
1. Identity-proofing of registrant	
	Business Practices: DNREC will be receiving Hazardous Waste Handlers Notification, Hazardous Waste Annual Report, Asbestos Notification, Notice of Intent (NOI), Discharge Monitoring Reports (DMRs) and National Emissions Inventory (NEI) (referred to collectively as "REPORT(S)" hereafter) online using DNREC ORS. DNREC ORS will use a Subscriber Agreement for DMRs, Hazardous Waste Annual Report (priority reports) and Asbestos Notification and NEI (non priority reports). We will call these reports as "Group A Reports". 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. DNREC will review the information provided and perform additional identity proofing to the best of their ability. For Hazardous Waste Handler Reports and NOI reports (non priority reports) identity proofing based on the user's driver's license will be performed online. We will call these reports as "Group B Reports". For these reports the driver's license will be verified for all the attributes of the certifier against the Delaware DMV database using web services. The attributes collected are: License number, State issuing the license, Name and address exactly as printed on the license, Date license issued and date it expires. The submitters of these reports are mostly one time users and hence use of subscriber agreement will be impractical. However, they will be accepting online all the terms using the same Subscriber Agreement as described in 1b-alt.by a checking a box on the web form. Initially online reports will be restricted to holders of Delaware licenses. However, we will attempt to make arrangements with other nearby states to get their drivers' license data so we can accept data online reports from holders of licenses of those states.
	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): • A draft copy of subscriber Agreement is attached – Attachment 1 • A printout of the application for Group B reports is attached.- Attachment 2
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 DNREC to assure the requested access is appropriate for the user.

	System Functions: DNREC ORS 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 DNREC 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 (for Group A Reports) in an online form. The user will then print, sign, and mail the subscriber form to DNREC. The user's electronic signature device will not be able to sign electronic documents until the Subscriber Agreement has been received by the DNREC and it has verified the

information (see Business Practices).
The online 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 facility whose reports the user is requesting signing privileges.
4. For each facility whether the user has direct authority under the rules to sign the Reports 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 DNREC any evidence of the loss, theft, or other compromise of the user account password.
c. Notify DNREC if the user ceases to represent any of the requested facilities as the submitter for the organization's electronic reports to DNREC ORS 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 DNREC ORS 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.
DNREC ORS will automatically validate that the requested permits/reports are valid for electronic reporting. 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_Supporting_.doc.
The document titled DNREC ORS CROMERR System Checklist Supporting Documentation, under paragraph Item 1b-alt contains the required information. To elaborate further the subscriber agreement is stored by the DNREC Program administering the particular online report in the facility's file in the filing cabinet which is securely locked.
The draft subscriber Agreement is attached.- Attachment 1

2. Determination of registrant's signing authority

Business Practices:
DNREC must receive a signed Subscriber Agreement from each user that is requesting the ability to sign Group A Reports. DNREC 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/reports. Once verification is complete, the DNREC will assign the user's account the appropriate Group A Reports signatory permission.

The respective programs responsible to administer the Group A REPORTS using DNREC ORS will also receive signed subscriber agreements from individuals requesting the ability to sign the Group A Reports electronically. Upon receipt of the subscriber agreement, each program will verify the signatures on the subscriber agreement through direct contact with the facility. This can be either through a phone call or an inspector verifying the signature during an inspection of the facility. Each program will verify that the "Cognizant Official" is in its database for every report the user includes in the subscriber agreement and that has been verified by the appropriate program. Each program will retain a paper copy of the subscriber agreement on file according to item #1b-alt. Upon verification, the Administrator of each report will assign appropriate level of access in DNREC ORS.

For the Group B Reports signing authority will not be verified but a statement will be obtained online as to the signing authority of the user.

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

Supporting Documentation (list attachments):
See attachment CROMERR_checklist_Supporting_.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 for Group A Reports. See supporting documentation for additional business processes relating to this item.
For Group B Reports the business process is described in Item 1.

System Functions:
I. DNREC ORS provides the following mechanisms to securely issue signing credentials:
1. The Subscriber Agreement (for Group A Reports) contains language requiring the user to protect their signing credential, not to share it with anyone else, and report any compromise to the DNREC (see Item 4 for more information on the contents of the signature agreement). For Group B Reports user will be asked online to agree to the same language.
2. The account creation process provides numerous levels of verification. The attached Registration Flow document provides the overall flow for creating a new DNREC ORS 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 DNREC ORS through the use of an algorithm that generates a random, globally unique key. For example, a custom application 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[1]) to generate the actual key. The Verification Key will only be valid for only 10 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 DNREC ORS 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 DNREC ORS 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 DNREC program 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. The system will check to comply with this requirement and reject those not meeting the requirements reminding the user of the password

requirements. There is no manual check for passwords.
g. Only verified accounts have access to DNREC ORS beyond the verification page. Verified accounts have limited access to DNREC ORS until DNREC 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 is created using the custom application for each user and stored in the DNREC ORS database. While the likelihood of custom application generating the same random salt for multiple users is remote, DNREC ORS 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 password salt is not communicated to the user. So there is no question of unauthorized disclosure or interception Password salts are stored in the database unencrypted. So no compromise is expected .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 DNREC ORS Registration Flow Diagram contains the overall flow for creating a new DNREC ORS 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 DNREC ORS prior to the intended registrant he/she would still need to complete, print, sign, and mail the Subscriber Agreement to the DNREC before he/she would be able to submit a fraudulent Group A Reports. This would require the malicious user to know the applicable permit IDs for the user, and submit a forged Subscriber Agreement. For Group B Reports this will not be feasible.
c. If a malicious user performed the steps in (b), the intended recipient would be able to detect the compromise for Group A Reports. 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. For more information on the verification business process, see Item 1b-alt. II. DNREC ORS provides additional credential protection throughout the lifetime of the account:
1. DNREC ORS requires all users to provide the answer to five security questions at the time a user registers to use the system. Security questions are answered online. All communications on the Internet take place using Secure Socket Layer v3 or Transport Layer Security v1. So there can be no compromise by interception. The list of available questions will be provided by DNREC ORS. 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 DNREC ORS 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, DNREC ORS will randomly (via **Custom application**) 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 DNREC ORS. Users must reenter the account's password and answer the security question prior to changing any account information. All of these take place online. All such transactions occur using Secure Socket Layer v3 or Transport Layer Security v1. If a person forgets his/her password he/she makes a request for a new password online by clicking the "forgot password" link on the login page. The person is prompted to answer a security question. If answered correctly a password is generated by the system and sent to the person's email address. When the person logs in using the new password he/she is required to change the password. The entire ORS application uses SSL, so all such transactions are secure.

3. DNREC ORS 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. Password reset is required every 90 days.

4. There will be a "user profile" tab in the ORS. When a person is logged in he/she can change his/her last name, address, phone number and email address using the profile tab. Since the user has to log into the system to make such changes no interloper can make such changes. An email will be sent to the new and old email addresses. If the actual account owner did not change the email address he/she can get the account locked out at this time.

5. An Account is locked after three unsuccessful login attempts, three unsuccessful attempts to sign REPORTS or three unsuccessful attempts to change account information within a 24 hour period. The account will typically be locked when the user forgets either the user ID or password. The user can use the "forgot password" link on the login page to unlock the account. When the user clicks the link the user is prompted to answer a security question. If this is answered correctly the user is emailed his/her user ID and a new password generated by the system. The account is unlocked at this point. When the person logs in using the new password he/she is required to change the password. The entire ORS application uses SSL, so all such transactions are secure. Even when a person calls in he/she is directed to login page. If the person cannot remember the security question answer he/she will have to reregister. Once locked:

i. The account cannot be used to log in to DNREC ORS.

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 DNREC 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 DNREC to have the account unlocked.

iii. An email is sent to the appropriate DNREC program contact responsible for the report describing the potential problem.

6. When a locked account is unlocked, the process outlined in 4.ii above 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 DNREC ORS until he/she visits the verification page and reset the account password.

- **Supporting Documentation (list attachments):**
  See DNREC ORS Registration Flow Diagram.jpg
- See attachment CROMERR Checklist DNREC ORS Supporting.doc
- Example of email from DNREC ORS on initial email during registration- Attachment 3
- Example of DNREC ORS email notification of locked account-attachment 4

4. Electronic signature agreement

Business Practices:
See Item 1b-alt

System Functions: DNREC ORS will use a Subscriber Agreement, which is defined as "an electronic signature agreement signed by an individual with a handwritten signature" for Group A Reports. The content of the Subscriber Agreement is described in Item 1balt.
For Group B Reports after online verification of identity using driver's license content of the Subscriber Agreement will be provided online for acceptance by the signer. This is detailed in

	Item 1.
	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 DNREC ORS Signature Process Flow Diagram illustrates the overall flow.

DNREC ORS allows users to submit multiple reports within a single transaction. However, DNREC ORS will create a unique Copy of Record (COR) for each report that is submitted. DNREC ORS also allows users to upload supporting documentation (i.e., attached files) that should be associated with the reports. 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 REPORT**.** The data document is A PDF document. The document includes, at a minimum:

1. All the user-provided data for the REPORTS
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 REPORTS displayed on the Verification page he/she intends to sign (e.g., through a checkbox next to each REPORT)

• DNREC ORS 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 REPORTS

• If the user enters the wrong password or answer to the secret question 3 times within a 24 hour period, the account will be locked and cannot be used until it is unlocked. See Item 3 for more information on how the account can be unlocked.

Hash Algorithm

• DNREC ORS uses SHA-256 to generate all hash values. This is the current approved FIPS standard[3].

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 REPORTS are submitted by the user at the same time, each REPORT within the submission will

have the same confirmation number.

Submission Receipt

• A submission receipt is created for each REPORT 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 ("Account Login" is the Login ID of the person. Its purpose is another parameter in the submission receipt along with the name of the person signing the document.)
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 REPORT. It contains
1. Data document
2. Attached files (if applicable)
3. Submission receipt

COR Signature

• Each DNREC ORS installation will have an RSA 1024 bit asymmetric key that will only be used for digital signatures. The RSA 1024 key function is provided by the certificate generated in the Microsoft SQL server using the syntax CREATE CERTIFICATE. It is stored in the SQL Server box. Only authorized individuals such as the data base administrator, his/her backup, the developer of the DNREC ORS and the network administrator will have access to the key. The SQL Server generated certificate is associated with the RSA key. Life span of the certificate will be 5 years. Since the certificate is used to sign documents on the server the issue of a recognized certificate authority such as Verisign does not arise. The server is located in the DMZ with appropriate physical security with key entry system (e.g., not used to establish SSL connections).
• DNREC ORS will use its private key to digitally sign[3] the CORs. The signature will be executed against a message digest created from the COR using the SHA-256 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 DNREC ORS RSA key.
4. Instructions to download the COR.
5. Instructions to view the COR online.

COR Alteration Protection

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

Use Case A. Signatory Falsification

Description: A signatory claims that DNREC ORS 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 DNREC ORS 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 DNREC ORS 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 DNREC ORS private key will be protected from unauthorized access by storing it in a secure location on the DNREC ORS server. Physical access to the server will be restricted as specified in Item 20. • A DNREC ORS administrator is required to specify which key pair on the server DNREC ORS will use for digital signatures. DNREC ORS will log any changes made to the key/pair used by DNREC ORS for signing CORs. This log will identify the key/pair that was changed, the date and time of change, and administrator making the change. This is an automatic system function. Only authorized individuals such as the data base administrator, his/her backup, the developer of the DNREC ORS and the network administrator will have access to the log. As for the user login the name of the user, user ID and the date and time of the user login is kept in the log. These strategies protect DNREC ORS 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 DNREC ORS. **Use Case B. DNREC Staff Falsification** *Description*: A DNREC staff member alters the COR in DNREC ORS 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 DNREC ORS 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 DNREC ORS private key in order to generate a new signature. The key pair can only be registered for use with DNREC ORS through direct access to the DNREC ORS server. Physical access to the server will be restricted as specified in Item 20. Additionally, a DNREC ORS Administrator must configure DNREC ORS to use the registered key pair. • DNREC ORS 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 DNREC ORS 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 DNREC ORS signature without the private key. The fact that the Signatory has a valid signature would provide strong evidence that the data in DNREC ORS had been altered. To alter the submission without detection the staff member (or members) would require access to the database, the DNREC ORS server, tape backups, and the email system. The staff member would also need enough detailed knowledge of DNREC ORS 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 DNREC ORS 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 DNREC ORS without the knowledge of the Regulatory Authority or signatory. A possible scenario includes a group attempting to alter a submission from being compliant to noncompliant 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 DNREC ORS 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 REPORTS 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 REPORTS may be displayed in a summary format with the ability for the user to expand the REPORTS to display all the information. 2. Links to download and view any documents that were attached to the REPORTS 3. Checkboxes to confirm selection of the Reports 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): • Example printout of a submitted document in human-readable format – Attachment 5
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 for Group A Reports or per the online certification for Group B Reports). 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 as follows: *I certify (that I have not violated any term in my Electronic Signature Agreement) 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. I had the opportunity, at the time of signing, to review the content or meaning of the this certification statement, including any applicable provisions that false certification carries criminal penalties
	Supporting Documentation (list attachments): • Example print out of certification statement – Attachment 6

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 DNREC ORS. 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. The data is transmitted in the SSL using TCP/IP protocol. It is this protocol's function to check transmission errors and correct them. The system does not provide any error notifications. When a document is received by the DNREC ORS the protocol guarantees that it is an error free document. The signer gets an email when a document is received by ORS. If the signer does not receive an email it is an indication that the document was not received by ORS and the program will investigate the cause. 3. The information in the Data document used for the verification page (see Item 5) comes from data already stored in the DNREC ORS 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 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 DNREC ORS private key. This protects against users modifying the COR and attempting to claim the data were altered in DNREC ORS (see Use Case A in Item 5) 7. The validity of the signed COR can be determined using the DNREC ORS public key. This assures that the DNREC ORS 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 DNREC ORS. This will be documented in the DNREC ORS 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 REPORTS 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): • Example print out of Copy of Record viewed online and downloaded copy – Attachment 7

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: 1. Data document in PDF format if the data was entered online DNREC's system or as XML document if the document was uploaded. For XML files there will be an XSL style sheet that will enable the submitter to convert the files into a human readable format for reviewing the document before submittal. 2. 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: DNREC ORS 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 report can view the CORs for that report. They can view submitted CORs by logging into DNREC ORS and searching for CORs for the specified permit. The COR can be presented in a human-readable format in two ways: 1. Download - DNREC ORS allows users to download the COR. After unzipping the COR, the user can view the Data document in PDF and all the supporting documents that were attached to the REPORTS submission. 2. Online Viewing - DNREC ORS would provide a mechanism to allow user to view the contents of the COR online. DNREC ORS would automatically unzip the submission zip file to retrieve the files. The user can view the Data document in PDF, and download any supporting documents that were attached to the REPORTS 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. When the signer gets an email after submission of a report it will contain a link for repudiation. The page from the link will contain contact information for Program Administrator for repudiation. The repudiation will occur online after the Program Administrator has given permission to signer to resubmit correct data. The Program Administrator unlocks the record; the signer logs in and corrects the data and resubmits the report. This will invalidate the old copy of record and a new copy of record is created. DNREC ORS allows users to submit corrections to REPORTS previously submitted through DNREC ORS. Users can also replace attachments that were previously submitted. Therefore, users should not repudiate a DNREC ORS submission due to incorrect data. Instead, he/she should submit corrected REPORTS**,** which would generate a new COR. In this manner, the entire history of the REPORTS**,** including all corrections, will be documented. In all cases all the previous versions of the COR (including the original and all the subsequent corrections) will always be retained identified by the version number and date of submittal.

	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 DNREC. After calling DNREC, the extent of the compromise will be assessed to determine whether any additional submissions need to be repudiated. The signatory and DNREC will also investigate how the account may have become compromised in order to prevent future occurrences. The DNREC will flag each fraudulently submitted COR as repudiated. To lock his/her account the user logs into the ORS and checks a box in the Profile tab to lock the account. This will send an email to the user's email account stating that the account has been locked. Once locked, only a DNREC Administrator can unlock an account.
	System Functions: The help system will document the repudiation process. The system allows DNREC 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 REPORTS, 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: DNREC ORS provides multiple mechanisms to prevent accidental submissions: 1. DNREC ORS performs a QA analysis on all REPORTS to validate that all required data points are provided. Only REPORTS that pass the QA analysis can be submitted. 2. The DNREC ORS submission process uses a multi-step approach to reduce the likelihood of accidental submissions. a. Users must select the REPORTS 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 REPORTS 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 DNREC ORS. DNREC ORS 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: DNREC ORS sends an acknowledgement email to the email address on file for the submitter after every submission. The email will contain the date and time of submittal of the report so that the submitter can identify the report in question. An email log is kept to track that the acknowledgement was sent. The log will contain information such as user name, user ID, date and timestamp.
	Supporting Documentation (list attachments): • Example email notification acknowledging receipt of report – Attachment 8

Signature Validation (e-signature cases only)

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

13a. Determination that credential is authentic

	Business Practices:
	System Functions: DNREC ORS 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: DNREC ORS 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 REPORTS and the user will be contacted to address the situation.
	System Functions: DNREC ORS includes functions that allow DNREC ORS Administrators and users to detect credential compromises. The signing process includes answering a challenge question as a second factor, the answer to which is only known to the signer. This provides independent evidence that the signer's password remains within the control of the signer who created and registered it. See Item 15 for a description of these functions. DNREC ORS 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 REPORTS were 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 DNREC ORS Administrators use to grant signatory authority to DNREC ORS users.
	System Functions: The DNREC ORS authorization system includes a "submit" role that grants permission for a user to sign a REPORTS . The "submit" role includes signatory authority. This role is associated with a user and each permit for which he/she has signatory authority. DNREC ORS uses the authorization system to determine whether a given user is authorized to submit a given REPORT(S). A responsible official of a firm can request that the signature authorization of a signer be revoked. If requested over the phone a written request will have to be made to confirm the initial request. An email will go out to the authorized signer's email following the revocation. The signer can challenge this if the revocation is not genuine and the Program receiving the report will conduct an enquiry.
	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 REPORTS , and the user will be contacted to address the situation. Our plan is to review the results once a quarter for a sample of users

	System Functions: DNREC ORS includes functions that allow DNREC ORS Administrators to detect the possibility that a user's device has been compromised: 1. Each time a user logs in to DNREC ORS, 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. DNREC ORS will only allow a user to maintain a single concurrent DNREC ORS 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. DNREC ORS will include fraud analysis functionality, in which the logs are periodically analyzed for irregularities. Irregularities will be flagged for DNREC ORS Administrators to investigate and take further action, if appropriate. The irregularities DNREC ORS 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 REPORTS every month for the past 6 months, but then submits 50 in one month. DNREC ORS includes functions that allow DNREC ORS users to detect the possibility that their account has been compromised. 1. After each REPORTS is submitted the submitter is sent an email acknowledging the submission. 2. After logging in to DNREC ORS, 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 DNREC ORS Supporting.doc for the guideline regarding the timeliness of administrator action when account compromise suspected.
	System Functions: Users are able to lock their account and DNREC ORS 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 cannot be used to sign a REPORT or log into DNREC ORS.
	Supporting Documentation (list attachments):
17. Confirmation of signature binding to document content	
	Business Practices:

	System Functions: DNREC ORS 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: DNREC ORS 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: **PDF Documents** The Data document is a PDF file **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: DNREC ORS generates the COR during the submission process. The COR is available for review using DNREC ORS by registrants with the authority to view CORs for the specified permit. Internal staff is also able to view CORs. DNREC ORS 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 DNREC ORS for the entire length of time for which they are maintained in DNREC ORS. See Item 20 for the retention schedule.
	Supporting Documentation (list attachments):
20. Maintenance of copy of record	
	Business Practices:
	System Functions: **CORs** DNREC ORS CORs are stored/retained in the DNREC ORS 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 DNREC ORS. The CORs can be searched, viewed, and downloaded as specified in Item 19. DNREC ORS will maintain CORs per the retention policy or the regulations of each DNREC Program receiving the REPORT(S). See the supporting documentation for the exact length of time CORs will be stored. **Logs** The DNREC ORS 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, DNREC ORS 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. The backups are stored for ever. **Physical Security** See the supporting documentation for the more information on the physical security.
	Supporting Documentation (list attachments): See attachment CROMERR Checklist DNREC ORS Supporting.doc.

References:

[1] NIST Hash Function Policy:
http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NIST_Policy_on_HashFunctions.htm

[2] Federal Information Processing Standards (FIPS)-approved algorithms for generating Message Digest:

http://www.csrc.nist.gov/CryptoToolkit/tkhash.html
[3]FIPS-approved algorithms for generating/verifying digital signatures:
http://www.csrc.nist.gov/CryptoToolkit/tkdigsigs.html

Attachment 1

Example of Subscriber Agreement

SUBSCRIBER AGREEMENT
FOR SUBMITTING DATA ELECTRONICALLY TO THE DEPARTMENT OF NATURAL RESOURCES AND ENVIRONMENTAL CONTROL (DNREC) – ASBESTOS PROGRAM
(DRAFT)

In accepting the electronic signature credential issued by the Department of Natural Resources and Environmental Control (DNREC) to sign electronic reports submitted to DNREC's Online Reporting System (ORS):

Company Name:

Address:

City, State, Zip:

Phone Number:

Fax:

Email Address:

Facility Name:

Facility Address:

Facility City, State, Zip:

Facility ID:

I,

I (Insert Name of authorized official)

(1) Agree to protect the signature from use by anyone except me, and to confirm system security with third parties where necessary. Specifically, I agree to maintain the secrecy of the code where the signature is based on a secret code;
(2) Understand that the immediate Supervisor or Witnessing Official who signs below will be contacted by the DNREC and asked to validate my employment at the Corporation Name listed above;
(3) Understand and agree that I will be held as legally bound, obligated, or responsible by my use of my electronic signature as I would be using my hand-written signature, and that legal action can be taken against me based on my use of my electronic signature in submitting an electronic document to the DNREC's Online Reporting System;

(4) Agree never to delegate the use of my electronic signature or make my signature available or use by anyone else;
(5) Understands that whenever I electronically sign and submit an electronic document to the DNREC Online Reporting System, acknowledgements and a copy of my submission will be made available to me;
(6) Agree to review the acknowledgements and copies of documents I electronically sign and submit to the DNREC Electric Reporting System;
(7) Agree to report to the DNREC, within twenty-four hours of discovery, any evidence of the loss, theft, or other compromise of any component of my electronic signature;
(8) Agree to report to the DNREC, within twenty-four hours of discovery, any evidence of discrepancy between an electronic document I have signed and submitted and what the DNREC Electronic Reporting System has received for me;
(9) Agree to notify the DNREC if I cease to represent the regulated entity specified above as signatory of that organization's electronic submissions to the DNREC Online Reporting System, as soon as this change in relationship occurs and to sign a surrender certification at that time.

E-mail Address for DNREC Online Reporting System correspondence:

Name of electronic signature holder:

Signature of electronic signature holder:

Official Title:

Date:

Authorization by Immediate Supervisor or Witnessing Official:

I, (insert name) acknowledged that the individual named above works at/for _____ and is authorized to submit documents on the company's behalf.

_____ _____

Signature of Immediate Supervisor or Witnessing Official Date

_____ _____

Official Title Date

Definitions

1. Electronic signature means any information in digital form that is included in or logically associated with an electronic document for the purpose of expressing the same meaning and intention as would a handwritten signature if affixed to an equivalent paper document with the same reference to the same content. The electronic

document bears or has on it an electronic signature where it includes or has logically associated with it such information.

2. Electronic signature credential refers to the token held by the individual user that is used to electronically sign electronic submissions. In the case of Asbestos Reporting, the electronic signature credential consists of the re-entry of the DNREC Online Reporting System password that the Asbestos Reporting Certifier established when they create their DNREC Online Reporting System account. This answer will be stored by DNREC Electronic Reporting System. The password will be asked each time a user attempts to certify an Asbestos Report electronic submission through DNREC Online Reporting System and the correct answer will allow for the certification and submission of the Asbestos Reporting file to DNREC.

PLEASE MAIL THIS DOCUMENT AS SOON AS POSSIBLE TO:

Department of Natural Resources and Environmental Control
715, Grantham Lane, New Castle, DE 19720
Attention: Colin Gomes

Attachment 2

Example printout of the application for Group B reports

Group B Report Signer Information (NOI, Hazardous Waste Notification)

Please enter information exactly as it appears in your Driver's License.

Name:

Address1:

Address2:

City:

State:

Zip:

License No.

License Issue date:

License Expires Date

Attachment 3

Example of the email to complete registration

DNREC ORS (DNREC)

From: DNREC ORS (DNREC)
Sent: Tuesday, September 30, 2008 2:58 PM
To: jmorgan@dupont.usa.com1
Subject: Registration in DNREC ORS

Dear Mr. Morgan,

To complete the registration on this site, please click on the link below

<aref="http://dnrecapdevel01/CROMERR/frmVerificationPage.aspx?verificationcode=hr0h5upBM0J+jUq10ev9mNCw47L5bGd1RdOBxhpsnB0=">Click here to complete your EMail verification.

Thank you.

DNREC Online Reporting System

Attachment 4

Example of the email notifying registrant of locked account

DNREC ORS (DNREC)

From: DNREC ORS (DNREC)
Sent: Monday, September 29, 2008 12:58 PM
To: jmorgan@dupont.usa.com1
Subject: Locked Account

Dear Mr. Morgan,

You have either used the wrong User ID or the password three consecutive times in the last 24 hours trying to log into the DNREC Online Reporting System. Therefore your account has been locked out. Please either contact your Program Administrator in DNREC or click the "Forgot Password" link in the login screen of the Online Reporting System to activate your account.

Thank you.

DNREC Online Reporting System

Attachment 5

Example of a submitted document in human readable format

Notification of Demolition or Renovation

Notification ID and Dates
Notification ID: DEN080548A **PostMark Date:** 09/22/2008 **Resubmit Date:**

Facility Information
Owner: A.I. DuPont Children's Hospital
Address: 1600 Rockland Road
City: Wilmington **County:** New Castle **State:** Delaware **Zip:** 19899
Contact: Scott Capaldi **Telephone:** 302-651-6942 **E-mail ID:** Scott.Capaldi@dupont.us.com

Removal Contractor
Contractor: Marcor of Pennsylvania
Address: 540 Trestle Bridge Road
City: Downingtown **County: State:** PA **Zip:** 19335
Site Contact: Steve Cacciavillano
Telephone: 610-269-3250 **E-mail ID:** deweesl@marcor.com

Demolition Contractor/Other
Contractor: Not Applicable N / A
Address: N / A
City: new castle **County: State:** DE **Zip:** 19720
Site Contact: Steve Cacciavillano
Telephone: 302-555-1212 **E-mail ID:**

Certified Professional Services Firm
Services Firm : Environmental Management International Inc.
Address: 34 East Germantown Pike
City: East Norriton **County: State:** PA **Zip:** 19401
Site Contact: Ray Giordano **Telephone:** 856-229-5369 **E-mail ID:** rayjg54@yahoo.com

Type of Notification / Operation
Type of Notification: Original
Type of Operation: Renovation (NESHAP)
Is Asbestos Present?: Yes

Facility Description
Building Name: DuPont Children's Hospital
Address #1: 1600 Rockland Road
Address #2: PO Box 269
City: Wilmington **County:** New Castle **State:** Delaware **Zip:** 19899
Site Location: 2nd Hall **Public Use?:** Yes
Building Size: 250000SF **Number of Floors:** 4
Age in Years: 50
Present Use: Hospital **Prior Use:** Hospital

Procedure Used to Identify the Presence of Asbestos
Procedure / Analytical Method Used: Inspection and PLM Test Report

Amount of Regulated Asbestos-Containing Material (RACM) to be Removed

Approximate Amount of Asbestos	RACM to be Removed	Nonfriable Asbestos Not to be Removed				
		CAT I	CAT II	CAT I	CAT II	Unit
Pipes:						
Surface Area:				1000		Sq. ft

Volume of Facility Component:						

Scheduled Dates and Working Hours

Scheduled Dates of Asbestos Removal/Demolition/Renovation:
Start: **10/11/2008**
Finish: **10/13/2008**
Scheduled Working Hours (Shift Hours):
Start Hour(HH:MM):**07:00**
Finish Hour(HH:MM):**17:00**

Description of Planned Demolition or Renovation work, and Methods To be Used

Description: removal and disposal of VAT/mastic

Description of Engineering Controls and work Practices to be Used to Control Emissions of Asbestos at the Demolition or Renovation Site

Description: segregate area, machine for tile, solvent for mastic, HEPA vac clean-up, maintain wet at all times

Waste Transporter

Waste Transporter #1: Marcor of Pennsylvania
Address:540 Trestle Bridge Road
City: Downingtown **County: State:** PA **Zip:** 19335
Telephone:610-269-3250 **E-mail ID:**deweesl@marcor.com
Waste Transporter #2: Service Transport Group Inc
Address:58 Pyles Lane
City: New Castle **County: State:** DE **Zip:** 19720
Telephone:302-778-5930 **E-mail ID:**

Waste Disposal Site

Site Name: Sanitary Landfill**EPA**
Certification Number:100277
Address:901 Tyrol Blvd
City: Belle Vernon **County:** Fayette **State:** Pennsylvania **Zip:** 15012
Site Contact: Clement Gigliotti
Telephone: 724-929-7694 **E-mail ID:**

Government Agency That Ordered Demolition

Agency Name: Title:
Authority:
Date of Order: Date Ordered to Begin:

Emergency Renovations

Emergency Renovation? No
Emergency Date:
Hour(HH:MM):
Description of Sudden, Unexpected Event:
Explanation of how the Event caused unsafe conditions, or a serious disruption of industrial operations:

Description of procedures to be followed in the event that unexpected asbestos is found or that previously non-friable asbestos material becomes crumbled pulverised, or reduced to powder

Description: wet materials, post signs, HEPA vac clean-up, alert generator

General Comments
Comments:

Signature
Signature:

Attachment 6

Example printout of Certification Statement

I certify that I am the authorized person to sign the document as per the Electronic Signature Agreement I signed and submitted to the Department of Natural Resources and Environmental Control. I agree that providing my account password to sign the document constitutes an electronic signature equivalent to my written signature.

I certify that I have not violated any term in my Electronic Signature Agreement, 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. I had the opportunity, at the time of signing, to review the content or meaning of this certification statement, including any applicable provisions that false certification carries criminal penalties.

Agree | Disagree

Attachment 7

Example Copy of Record

Notification of Demolition or Renovation

Notification ID and Dates
Notification ID: DEN080548A **PostMark Date:** 09/22/2008 **Resubmit Date:**

Facility Information
Owner: A.I. DuPont Children's Hospital
Address: 1600 Rockland Road
City: Wilmington **County:** New Castle **State:** Delaware **Zip:** 19899
Contact: Scott Capaldi **Telephone:** 302-651-6942 **E-mail ID:**

Removal Contractor
Contractor: Marcor of Pennsylvania
Address: 540 Trestle Bridge Road
City: Downingtown **County: State:** PA **Zip:** 19335
Site Contact: Steve Cacciavillano
Telephone: 610-269-3250 **E-mail ID:** deweesl@marcor.com

Demolition Contractor/Other
Contractor: Not Applicable N / A
Address: N / A
City: new castle **County: State:** DE **Zip:** 19720
Site Contact: Steve Cacciavillano
Telephone: 302-555-1212 **E-mail ID:**

Certified Professional Services Firm
Services Firm : Environmental Management International Inc.
Address: 34 East Germantown Pike
City: East Norriton **County: State:** PA **Zip:** 19401
Site Contact: Ray Giordano **Telephone:** 856-229-5369 **E-mail ID:** rayjg54@yahoo.com

Type of Notification / Operation
Type of Notification: Original
Type of Operation: Renovation (NESHAP)
Is Asbestos Present?: Yes

Facility Description
Building Name: DuPont Children's Hospital
Address #1: 1600 Rockland Road
Address #2: PO Box 269
City: Wilmington **County:** New Castle **State:** Delaware **Zip:** 19899
Site Location: 2nd Hall **Public Use?:** Yes
Building Size: 250000SF **Number of Floors:** 4
Age in Years: 50
Present Use: Hospital **Prior Use:** Hospital

Procedure Used to Identify the Presence of Asbestos
Procedure / Analytical Method Used: Inspection and PLM Test Report

Amount of Regulated Asbestos-Containing Material (RACM) to be Removed

Approximate Amount of Asbestos	RACM to be Removed	Nonfriable Asbestos Not to be Removed				
		CAT I	CAT II	CAT I	CAT II	Unit
Pipes:						

Surface Area:				1000		Sq. ft
Volume of Facility Component:						

Scheduled Dates and Working Hours

Scheduled Dates of Asbestos Removal/Demolition/Renovation:
Start: **10/11/2008**
Finish: **10/13/2008**
Scheduled Working Hours (Shift Hours):
Start Hour(HH:MM):**07:00**
Finish Hour(HH:MM):**17:00**

Description of Planned Demolition or Renovation work, and Methods To be Used

Description: removal and disposal of VAT/mastic

Description of Engineering Controls and work Practices to be Used to Control Emissions of Asbestos at the Demolition or Renovation Site

Description: segregate area, machine for tile, solvent for mastic, HEPA vac clean-up, maintain wet at all times

Waste Transporter

Waste Transporter #1: Marcor of Pennsylvania
Address:540 Trestle Bridge Road
City: Downingtown **County: State:** PA **Zip:** 19335
Telephone:610-269-3250 **E-mail ID:**deweesl@marcor.com
Waste Transporter #2: Service Transport Group Inc
Address:58 Pyles Lane
City: New Castle **County: State:** DE **Zip:** 19720
Telephone:302-778-5930 **E-mail ID:**

Waste Disposal Site

Site Name: Sanitary Landfill**EPA**
Certification Number:100277
Address:901 Tyrol Blvd
City: Belle Vernon **County:** Fayette **State:** Pennsylvania **Zip:** 15012
Site Contact: Clement Gigliotti
Telephone: 724-929-7694 **E-mail ID:**

Government Agency That Ordered Demolition

Agency Name: Title:
Authority:
Date of Order: Date Ordered to Begin:

Emergency Renovations

Emergency Renovation? No
Emergency Date:
Hour(HH:MM):
Description of Sudden, Unexpected Event:
Explanation of how the Event caused unsafe conditions, or a serious disruption of industrial operations:

Description of procedures to be followed in the event that unexpected asbestos is found or that previously non-friable asbestos material becomes crumbled pulverised, or reduced to powder

Description: wet materials, post signs, HEPA vac clean-up, alert generator

General Comments

Comments:

Signature

Signature:

1. Confirmation Number: 2008- DEN080548A
2. The hash of the data document:
3. Date/Time of the submission: 09-27-2008; 09:10:45
4. Identifying information from the signing account, including:

a. The user's full name: John Doe
b. Account Login : John.doe
c. Email Address: john.doe@company.com
d. Hashed Password (at time of signing):

5. IP of submitting computer: 126.67.76.21

Attachment 8

Example of an email notification of submission

DNREC ORS (DNREC)

From: DNREC ORS (DNREC)
Sent: Monday, September 29, 2008 12:58 PM
To: Scott.Capaldi@dupont.us.com1
Subject: Submission of Asbestos Report

Dear Mr. Capaldi,

Your Asbestos Notification Report # 2008- DEN080548A was received on 09-27-2008 at 09:10:45 hours. If you believe you did not submit this report you should repudiate the report by calling the number listed at https://www.cromerr.dnrec.delaware.gov/contacts. If you believe someone has compromised your account you must call immediately at the above number to lock your account.

You can view a "copy of record" of the report submitted by logging into your account and clicking the COR tab.

Thank you.

DNREC Online Reporting System