CROMERR System Checklist	
Item	
Registration (e-signature cases only)	
1. Identity-proofing of registrant	
	Business Practices: The San Joaquin Valley Air Pollution Control District (District) has developed the TVE System for electronically receiving the Report of Required Monitoring (RRM) and Annual Compliance Certification priority reports from regulated facilities. See Attachment #3 for system components. Per CROMERR 3.2000(b)(5)(vii)(A), the District will use a registration process to gather personal identification from TVE users (RO) to verify and establish their identity prior to being issue a digital signature. The District will also verify the RO's authority to represent and submit electronic reports on behalf of a facility. **Note:** Moving forward the RO and user may be used interchangeably where appropriate. The District has setup an online website to allow users to register for electronic reporting. The registration site gathers personal identifier information about the user that will later be used to verify user's identity and their authority to submit reports on behalf of a facility prior to being issued a digital signature. This information will also be used to generate a unique digital signature for the user after verifying their identity. The user is required to supply the following information during the online registration: • First and Last Name as listed in one of the forms of identification documents listed below. • Expiration Date of the selected form of identification document • A valid Email Address • Facility ID • Facility Name • Current Title/Position with Facility • Facility Contact Information • Digital Signature Password that must comply with the District's password requirements (8 case sensitive alpha-numeric characters minimum). This password is required so that the District may immediately generate a digital signature and protect it with this password upon verifying the user's identity. It is stored in encrypted form using the standard AES 256 encryption algorithm and is not displayed or shown visibly to anyone. Also required is a legible legally certified copy or original of one of the following forms of personal identification documentation: • Driver's License (Preferred) • State Identification Card • Passport The user may show their identification documents by way of walk-ins or mailing a certified copy of the identification to the District. Acceptable certifications should come from the issuing agency of the documentation such as Department of Motor Vehicles or the US Department of State. To verify a user's identity the District must: 1. Establish the user's identity by verifying information using government issued documents such as a driver's license, passport, or state identification card provided by the user. 2. Establish the user's authority to submit reports on behalf of a facility by contacting the

	facility to verify. The District also maintains a creditable database of authorized RO to facility assignments that can also be used for verification. District staffs who are assigned the role of the registration authority will initiate the identity proofing process upon receiving the registration information and identification documents from the user. They will try to match the registration data with the documentation provided. If the data matches then it satisfies the user's identity claim. See Attachment #2 for details on the identity verification procedures.
	System Functions: **Receipt an Online Registration Request** 1. The system checks to make sure the user (requestor) does not already have an existing account. If an existing account is found then a second account is not allowed. 2. If this is the first time a user has registered then a confirmation email is sent to the user with the registration information and further instructions to submit identification documents. 3. A notification email is sent to District staff letting them know of a new registration. At this point, District staff is ready to initiate the verification process once they receive the identity documentation from the user. See Attachment #1a,b,c for email samples.
	Supporting Documentation (list attachments): Attachment #1a,b,c –Registration Confirmation and New User Account Activation, New Registration Notification Email Messages Attachment #2 – Identity Proofing and Facility Affiliation Verification Procedure Attachment #3 – System Components Diagram Attachment #4 – Registration Process Diagram
1a. (priority reports only) Identity-proofing *before* accepting e-signatures	
	Business Practices: The District will not accept electronically signed reports from a user until they have gone through the registration process to verify their identity and confirm their authority to submit reports on behalf of a Title V facility. See item 1 on details to the identity proofing process. Once a user has gone through the verification process and the District has successfully verified their identity then a TVE website account and digital signature will be issued to the user. These two items establishes a trusted relationship between the user and the District. The District can now trust digitally signed reports from the user given that the reports were submitted using the TVE account and the digital signature is confirmed to be issued by the District. At a high level, the following identity proofing steps must be completed before the District will accept electronically signed reports from a user through the TVE website: 1. The user has registered with the District to submit electronic reports. 2. District staff is able to successfully verify the user's identity and authority to submit reports on behalf of a facility. 3. The District issues a TVE website account and digital signature to the user. Both protected with the password of choice only known to the user. 4. The user must login to the TVE website with valid credentials to submit electronic reports. A successful login vouches the user's ownership of the account. In addition to having valid credentials, the user is also required to answer correctly a random personal question chosen by them during the activation of their website account. 5. Only digital signatures issued by the District will be accepted on electronic reports.

6. The District must be able to successfully confirm the validity of the digital signature.
    a. Signature is not revoked
    b. Signature has not expired
    c. Signature is linked with the user account used in the submittal

System Functions:

The system will validate that the user is authorized to use the username and digital signature for electronic reporting. Successful validation establishes the identity of the user and their ownership of the credentials used for reporting.

Authenticating TVE Website Logons (Two step logon security)

1. Validate input username and password. The system will flag the account and lock it for 15 minutes if the username or password is incorrectly entered 3 times.
2. If username and password is correct then have the user validate a random personal security question.

Validating Digital Signatures on Reports

1. Validate to make sure user account used to submit the online report matches the account assigned to the digital signature used to sign the report. The system extracts the digital signature serial number and SHA1 thumbprint (unique identifiers for signature) on the report and tries to find a match within the TVE digital signatures database. Once a match is found the username associated with the matching data record is compared to the username used to submit the report. The digital signature on the report will be considered invalid if the system cannot find a match in the database.
2. The system will also validate the digital signature on the report by using the District's CA digital certificate to verify that the digital signature has not expired, is not revoked, and is issued by the District. The check is done by the system and if it fails then the user's digital signature is considered invalid.

Supporting Documentation (list attachments):
Attachment #1a,b,c –Registration Confirmation and New User Account Activation, New Registration Notification Email Messages
Attachment #2 – Identity Proofing and Facility Affiliation Verification Procedure
Attachment #3 – System Components Diagram
Attachment #4 – Registration Process Diagram

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:
The identity verification process will be completed by District staff members who are assigned the registration authority role for identity proofing. These members are not associated with the user in any way.

For users who wish to provide walk-in identification, they will be asked to provide a driver's license, state ID or passport. The staff will make a determination if identity verification pass or fail after sighting the person to make sure the person is the one shown in the photo ID. A photo copy will be required of the identification document so that a comparison can be done to make sure the online registration data matches the document. This is required as the registration data will be used to generate the digital signature.

For mail-in verification, the identification documents must be certified by the issuing agency. The identity verification in this case would be performed the issuer prior to providing a certified copy to the requester. Therefore, the District just requires the certified copy to confirm and use in validating

	the online registration data. Acceptable certifying agencies based on identification document type. • Department of Motor Vehicles (State ID and Driver's License) • US Department of State (Passport)
	System Functions: N/A
	Supporting Documentation (list attachments): Attachment #2 – Identity Proofing and Facility Affiliation Verification Procedure Attachment #4 – Registration Process Diagram

CROMERR System Checklist	
1bii. (priority reports only) Information or objects of independent origin	
	Business Practices: The documents required for the identity verification process are the original or certified copy provided by the Department of Motor Vehicles or US Department of State which are: • Driver's License (Preferred) • State Identification Card • Passport As required by CROMERR 3.2000(b)(5)(vii)(A), the identification documents listed above can only be changed by requesting authorization or be changed only through the issuing government agency. Any other type of document provided or certified by someone other than the listed government agencies will not be acceptable for identity verification.
	System Functions: N/A
	Supporting Documentation (list attachments): Attachment #2 – Identity Proofing and Facility Affiliation Verification Procedure
1b-alt. (priority reports only) Subscriber agreement alternative	
	Business Practices: N/A – See item #4
	System Functions: N/A
	Supporting Documentation (list attachments): N/A
2. Determination of registrant's signing authority	
	Business Practices: The registration authority staffs will contact a facility to confirm the user's authority to sign and submit reports on behalf of the facility. In many cases the user is the owner or the highest official operating the facility for a designated site which creates an implicit authorization. This type of scenario will still require verification by confirm with the facility and name and position title of the user. It will be the responsibility of the facility owner/highest official to report any changes in signatory authority to the District. Any major changes to the current authorized user such as legal name change or assignment of the reporting authority to a different person will require them to go through the identity verification process again. These actions are required under the Digital Signature Agreement document provided to users at the time of registration to ensure that user information is updated when it does change.

	System Functions: N/A
	Supporting Documentation (list attachments): Attachment #2 – Identity Proofing and Facility Affiliation Verification Procedure Attachment #5 – Electronic Signature Agreement

CROMERR System Checklist

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

Business Practices:

The TVE system implements digital signatures based on the Public Key Infrastructure (PKI) framework to protect them from compromise. PKI consists of programs, procedures, and policies that employ the Public Key Cryptography Standards (PKCS #12) and the X.509 digital certificate standard for secure communications. PKCS #12 defines the file format used to store the X.509 digital certificate (digital signature). X.509 defines the file format structure on encoding information inside a digital signature. Overall, PKI provides the infrastructure that identifies users, creates and distributes certificates, maintains and revokes certificates, distributes and maintains encryption keys, and enables technologies to communicate via encrypted communications.

The components of PKI are:

- **Certificate Authority** – An entity, normally a trusted third party, that issues digital certificates for identities. A certificate associates the identity of a person or server with the corresponding public key.
- **Registration Authority** – An entity that is responsible for the registration and initial identity verification of users who are issued certificates after a registration request is approved.
- **Certificate Server** – A machine or service responsible for generating and issuing digital certificates based on information provided at the registration process.
- **Certificate Repository** – A database that stores the digital certificates issued to users.
- **Certificate Services** – A services that provides functionality to validate digital certificates and provide signing and time stamping for use by applications utilizing digital certificates.

The District has chosen to be its own Certificate Authority (CA) and will also take on the roles and functions associated with the rest of the PKI components to ensure that digital signatures are issued in a secured manner. PKI helps to establish a repository of trusted digital signatures between the District and its regulated Title V facilities.

See attachment #7 for a visual diagram of the Title V PKI Infrastructure
See attachment #11 for PKI Whitepaper
See attachment #12 for PKI Infrastructure Abstract

In order to ensure that a user is entitled to use a digital signature at the time of signing, the digital signature is protected using a password (8 case sensitive alpha-numeric characters minimum) chosen by the user. This password will not be retained by the TVE system. The user will be responsible for keeping this password secured. This will ensure that only the user with the correct knowledge of the password will be able to use the digital signature to sign electronic reports. To determine if the digital signature is valid at the time of signing, the system performs a series of automated checks to answer the following questions:

- Was the digital signature issued by the District? [Yes]
- Was the issue of the digital signature authorized? [Yes]
- Has the digital signature been revoked for any reason? [No]
- Has the digital signature expired? [No]

- Was the signed report submitted through an authorized TVE website account assigned to the owner of the digital signature? [Yes]

The correct answers are listed above for valid digital signatures. If any of the answers are opposite to what is listed then the digital signature will be consider invalid.

In order to prevent the digital signature or signing device from being compromised at the time of signing, the District has provided a signing application tool to allow the user to perform offline signing. This means the signing process will be performed on the user's computer without any dependency on any remote services. This will ensure that no signing credentials are transferred over the Internet to limit any risks of compromise. The signing application tool ensures that the password required for the signing process is not stored on the user's computer. Its purpose is to take the password inputted by the user and validate the digital signature file also provided by the user. The password temporarily resides in memory only for the validation process.

See attachment #6 for screenshots of the signing tool application.

In order to issue digital signatures in a way that protects it from compromise, the District will generate an email message containing instructions to activate the user's assigned TVE website account and how to sign in to the website to download the digital signature. The web page containing the download link for the digital signature will be secured over an encrypted connection. The email message will be sent to the email address provided by the user during registration.

See attachment #1b for a sample account activation email message

System Functions:

Issuance of PKI Digital Signature and TVE Website Account

The user starts by going through the registration and identity verification process as described in item #1. The following information is collected from the user via the registration page to perform identity proofing.

- An ID number from one of the following forms of personal identification document:
  - Driver's License (Preferred)
  - State Identification Card
  - Passport
- First and Last Name as it appears on the identification document
- Expiration Date of the selected form of identification document
- A valid email address
- Digital signature password that must comply with the District's password requirements (8 case sensitive alpha-numeric characters minimum). This password is not available to anyone and is temporarily stored in the database as an encrypted field pending approval on a successful identity proof to move forward with creation of a digital signature. The password will be deleted from the system after creating the user digital signature.

The registration authority completes the identity proofing process and the CA issues a pair of electronic keys (Public & Private) that can be used to encrypt and sign electronic reports by the user. The keys are part of the digital signature which contains at the minimum these fields:

- Public and private keys
- User's full name
- Validity period of the certificate
- Issuer full Name
- Serial number of the digital certificate
- SHA1 hash of the digital certificate
- Authority Key Identifier

See attachment #8 for a full X.509 specification on the digital signature fields used.

The digital signature private key is encrypted using the user's digital signature password. The password is removed from the database. In order to use the digital signature for signing the correct password must be provided or the signing process will fail.

Following the digital signature creation is the TVE website account creation for the user. This account is provided for the specific purpose of submitting electronic reports, repudiating submittals, and downloading a copy of the user's digital signature. The account is protected with a random temporary password to be changed upon first logon. Also required upon first logon is the selection of 5 security questions from a pool of 15 to use as an additional security logon. The user will be required to answer a question picked at random upon each logon session. Failure to answer the question correctly will result in an access denied message preventing access to the website.

To deliver the digital signature and website account to the user, an automated email is generated with instructions on activating the web account and logging on to download the digital signature. It is sent to the email provided by the user during registration. Successful account activation requires that the user signs in using the username and temporary password provided in the email. A new account password (8 case sensitive alpha-numeric characters minimum) is required by the user in addition to selecting 5 security questions and answers from a pool of 15. Once the user completes the account activation they will be taken to the main page where a link is available to take them to a secured page over a Secured Socket Layer (SSL) connection to download their digital signature.

How does the District determine if the digital signature was valid at the time of signing?
There are multiple checks that are performed automatically by a Windows service to ensure that the digital signature is valid at the time of signing. All of the checks below must be successful to deem a valid electronic signature.

1. **Was the digital signature issued by the District? [Yes]**
   Compute a hash of the digital signature content for comparison. Then use the District CA's public key to decrypt the digital signature hash that was signed and encrypted using the CA's private key. If the result of the decrypted hash matches the computed hash then the certificate was issued by the CA.
2. **Was the issue of the digital signature authorized? [Yes]**
   Check to make sure the serial number & SHA1 hash of the digital certificate exists in the District's certificate database.
3. **Is digital signature revoked for any reason? [No]**
   Check the digital signature against the Certificate Revocation List (CRL) to make sure it wasn't revoked for any reason. (Compromised, Lost, Inactive digital signature...etc.)
4. **Has the digital signature expired? [No]**
   Check the digital signature's validity dates to make sure it is valid that the time of signing.
5. **Was the signed report submitted through an authorized account assigned to the owner of the digital signature? [Yes]**
   Check to make sure the signed report containing the digital signature was submitted using a valid TVE website account. The website account is issued with the digital signature and protected with a temporary password that is required to be changed upon initial login. The logon also requires the correct answer to a random security question chosen by the user from a pool of 5 during the account activation.

The correct answers are listed above for valid digital signatures. If any of the answers are opposite to what is listed then the digital signature will be consider invalid.

Steps taken to protect the digital signature from being compromised

1. First step is to protect the digital password from being compromise during online registration

submittal. The registration data is submitted to the District via an encrypted connection.
2. The digital signature password is stored in an encrypted format.
3. The digital signature password is not shown or available through any applications.
4. The digital signature password is deleted from the database after using it to encrypt and protect the user's PKI digital signature. Use of the digital signature to sign will now require that the correct password be provided.
5. The user's digital signature is countersigned by the District's CA root certificate. Thus enabling tamper detection afterwards which enables the District to easily check the digital signature's validity.
6. The digital signature can only be downloaded by logging onto the TVE website with the user's assigned website account and using the designated links to navigate to a secured page for the download. Logging on requires the correct password to the account and answering correctly 1 of 5 random security questions chosen during the activation of the account.
7. The digital signature password is not provided via the website. The system only uses it in the creation of the digital signature and deleted it afterwards. The user should be the only person with the knowledge of the password.
8. The user is supplied a digital signature user agreement and required to agree and follow all terms listed under the agreement. The agreement requires the user to protect their digital signature by not sharing it and reporting any compromised to the District. See Item #4 for the digital signature user agreement.
9. The District provided a PKI enabled electronic signature tool for the user to use in applying their digital signature to electronic reports. This will provide a safe mechanism for the user to use in signing electronic reports.

Supporting Documentation (list attachments):
Attachment #1b – Sample New User Account Activation Email Message
Attachment #6 - Digital Signer Application Screenshot
Attachment #7 – District's PKI Infrastructure Diagram
Attachment #8 - X509 Digital Signature Field Specification
Attachment #11 – PKI Whitepaper
Attachment #12 – PKI Infrastructure Abstract

4. Electronic signature agreement

Business Practices:
The TVE system uses the End User License Agreement (EULA) known as browse-wrap and click-wrap to form a binding contract each time the user uses the TVE system. The principle behind these two types of agreement is to bring the electronic signature agreement notice to the user's attention before the user logs into the TVE website or uses any of the related services.

See attachment #9 for information on browse-wrap and click-wrap agreements.

An electronic signature agreement link will be presented upon each logon into the TVE website account and upon receiving the initial instructions on activating the TVE website account and downloading the digital signature. The agreement will ensure that the user agrees to the terms and conditions when using the digital signature or associated electronic reporting services such as the TVE website and signing tool. At a minimum the agreement requires the user to:

- Take proactive measures to protect their TVE account and digital signature from compromise
- Report any changes in signatory status to the District
- Notify the District in the event of a compromised TVE account or digital signature
- Understand and adhere to the proper use of their digital signature and the legal bounds, obligations and responsibility associated with it.

See attachment #5 for the Digital Signature User Agreement

	System Functions: The system will display a link on the TVE website login screen to allow the user an opportunity to review the Digital Signature User Agreement prior to logon. The user must click on the agree checkbox to proceed. The Digital Signature User Agreement will also be included as a link in the account activation email that is sent to the user for initial account activation. User is required to review and agree to the terms when using the login screen to activate their account for the first time.
	Supporting Documentation (list attachments): Attachment #1b – Sample New User Account Activation Email Message Attachment #5 – Digital Signature User Agreement Attachment #9 – Browse Wrap Information Attachment #10 – TVE Website Login User Agreement Screenshot

CROMERR System Checklist

Signature Process (e-signature cases only)

5. Binding of signatures to document content

Business Practices:

When the TVE system receives electronic report data it parses it and puts the data into a human-readable format under the Portable Document Format (PDF) file type. PDF is the global standard for electronic information exchange invented by Adobe Systems Inc. PDF documents have built in support for digital signatures associated with PKI. CROMERR 3.2000(b)(5)(ii) requires that the system be able to show that the electronic document cannot be altered without detection once it has been electronically signed. In order to fulfill this requirement, the District will rely on the use of PKI digital signatures and its validation techniques to detect changes to a signed document.

See attachment #11 for PKI whitepaper.

PKI involves the use of two cryptographic keys, one private and one public. Information encrypted with one key in the pair can only be decrypted with the other key. The key pairs are generally embedded inside a protected computer file with personal details about the owner also known as a certificate. The private key is usually encrypted with a secret password only known by the owner. The TVE system uses the Public-Key Cryptography Standard (PKCS) #12 standard for storing or transporting a user's private keys or digital certificate. PKCS#12 provides high encryption for private keys, certificates and potentially other secret information. See attachment #30 – PKCS#12 Standard Syntax

Digital signatures use PKI technology to create legally binding proof of signature for online transactions or contracts. A digital signature is based on a mathematical transformation that combines the private key with the data to be signed in such a way that:

- Only someone possessing the private key can create the digital signature, providing authentication of the signing party.
- Anyone with access to the corresponding public key can verify the digital signature, enabling a non-repudiated transaction.
- Any modification of the signed data invalidates the digital signature, providing integrity proof for the parties involved.

Binding of signature to document and change detection of contents are enforced and guaranteed for both the user and District through the use of two digital signatures for signing. One is from the TVE system to certify the original document and the other is the user's signature. The certification signature is to prevent the user from changing the document before signing it. Any attempt to change the document before signing will invalidate the certification signature. The second signature is the user's signature. Any attempt to change the document after the user signs it will invalidate the user's signature.

Since both the user and certification signatures are issued by the District's CA, the can both be validated using the CA digital certificate. This ensures that the user identities on both digital signatures on the document can be attested.

System Functions:

Document Change Detection Process

How does it work?

1. Using special software provided by the District, a user creates a message digest or hash (a unique numerical representation) of the document, uniquely identifying the data to be signed.

2. The user uses their private key to encrypt the hash by providing the correct password to use the private key.
3. The encrypted message hash becomes the digital signature of the document.
4. The digital signature is embedded as part of the document and sent to the TVE system.

When the signed document is received:

1. The TVE system runs the document through the same hashing functions used by the user to obtain a hash value of the document.
2. The TVE system uses the user's public key to decrypt the signature and the hash value embedded in the document by the user.
3. A comparison of the hash value generated by the TVE system in step 1 and the hash value in step 2 is performed. If the hashes match, the integrity of the data is validated.
4. Next is to determine validate the digital signature certificate on the document to make sure the digital signature was issued by the District. See next section.

Signature Validation Process

When the TVE system receives a data submittal from a user it creates a human-readable copy of it known as the COR. This is a document file in the PDF file format. The COR is electronically signed using the Title V Data Certification digital signature. The COR is then emailed to the user for review and signing. See attachment #13 and #14 for sample email message and sample certified and signed COR. The certification signature is always located on the top right hand corner while the user's signature is always on the last page of the document. The user reviews and signs the COR using their digital signature. The signed COR is then submitted back to the TVE system where it is put through the signature validation process as described below.

The TVE system has a Windows service that requests functionality from a web service to perform the validation steps. The validation functionality is provided by a third party component called SecuredBlackBox by Eldos Inc.

Steps to perform validation

1. The Windows service will check the signed document to make sure it has at least two signatures. One for the data certification and one for the user consent.
2. Next the service will extract the digital signatures and pass them to the web service to validate if there were any changes detected. This process is outlined under the "How does it work?" section of the Business Practice.
3. Next the service will pass the digital signatures to the web service to check if they are valid at the time of signing. This process is also outlined in the system functions of item #3 and performs these checks.

- **Was the digital signature issued by the District? [Yes]**
  - *Compute a hash of the digital signature content for comparison. Then use the District CA's public key to decrypt the digital signature hash that was signed and encrypted using the CA's private key. If the result of the decrypted hash matches the computed hash then the certificate was issued by the CA.*
- **Was the issue of the digital signature authorized? [Yes]**
  - *Check to make sure the serial number & SHA1 hash of the digital certificate exists in the District's certificate database.*
- **Is digital signature revoked for any reason? [No]**
  - *Check the digital signature against the Certificate Revocation List (CRL) to make sure it wasn't revoked for any reason. (Compromised, Lost, Inactive digital signature...etc.)*
- **Has the digital signature expired? [No]**
  - *Check the digital signature's validity dates to make sure it is valid that the time of signing.*
- **Was the signed report submitted through an authorized account assigned to the owner of**

the digital signature? [Yes]

- *Check to make sure the signed report containing the digital signature was submitted using a valid TVE website account. The website account is issued with the digital signature and protected with a temporary password that is required to be changed upon initial login. The logon also requires the correct answer to a random security question chosen by the user from a pool of 5 during the account activation.*

The correct answers are shown for a check that determines a valid electronic signature. If any of the validation fails then the user will receive an email outlining the issue and to request corrections and resubmittal of a new signed COR document. See attachment #15 for sample email message for failed validations. If the validation passes then the user will receive an email notification that their COR was accepted. See attachment #16 for sample email message for successful validations.

Supporting Documentation (list attachments):
Attachment #11 – PKI Whitepaper
Attachment #12 – PKI Infrastructure Abstract
Attachment #30 – PKCS12 Standard Syntax
Attachment #13 – Data Submittal Confirmation Email
Attachment #14 – Sample Certified and Signed COR document
Attachment #15 – Sample Email Message for Failed Digital Signature Validation
Attachment #16 – Sample Email Message for Successful Digital Signature Validation
Attachment #17 - PKI Change Detection Process

6. Opportunity to review document content

Business Practices:
When the TVE system receives a data submittal from a user it creates a human-readable copy of it known as the COR. This is a document file in the PDF file format. The COR is then emailed to the user for review and offline signing. The email message lists the readily available and no cost Adobe Reader Software as the tool to use in viewing the COR. See attachment #13 and #14 for sample email message and sample certified COR. The user reviews and signs the COR using their digital signature. Also note that the user may open the PDF document at any time to review as long as they retain the email.

Another opportunity to review is presented when the user uses the District provided Digital Signature Application to sign the COR. A “Review” button is presented on the screen to allow the user to open the selected document as the first step before signing. See attachment #6 for the Digital Signature Application screenshot and “Review” button location.

The steps to electronically sign a document is labeled clearly on the Digital Signature Application screen as the following:

1. Where is the PDF Title V report you want to sign?
2. Where is your digital signature?
3. Please input your digital signature password.
4. Please verify the signature information before proceeding to sign.
5. Sign.

See Attachment #6 for a screenshot of the Digital Signature Application.

System Functions:
When the “Review” button in the Digital Signature Application is clicked it will launch the default PDF reader on the user’s computer and load the selected Title V report document (COR).

Supporting Documentation (list attachments):
Attachment #6 - Digital Signer Application Screenshot

7. Opportunity to review certification statements and warnings
Business Practices: When the TVE system creates the COR document it also appends a page titled "Certificate of Truth and Accuracy", which is the user signature page and lists the following certification and warning statement: *"By affixing my digital signature on this electronic Title V document, I declare under the penalty of perjury under the laws of the State of California that based on information and belief formed after reasonable inquiry, the statements and information provided in these document(s) are true, accurate, and complete. I understand that any false statements or information I provide may be punishable as a criminal offense."* This gives the user an opportunity to review the certification statement at the same time they review the COR as indicated in item #6. The same certification statement is also displayed to the user when the Digital Signature Application is used to sign the COR. See attachment #6 for screenshot of the pop up dialog containing the statement.
System Functions: When the system creates the COR it appends a page to the end of the document containing the certification statement for the user to review before signing the document. The same statements are also reiterated and shown when the user is ready to sign and clicks on the "Sign" button in the Digital Signature Application.
Supporting Documentation (list attachments): Attachment #6 - Digital Signer Application Screenshot

CROMERR System Checklist	
Submission Process	
8. Transmission error checking and documentation	
	Business Practices: To ensure that the data transmission contains error checking, the TCP/IP protocol is used for the delivery of data between the TVE server and the user client. TCP works by breaking the data to be transfer into small chunks known as data packets. Each data packet is appended with a TCP header segment that contains information about the destination of where the data is going, how to put the data packet back together with the rest of the other data packet to get the original data, and a checksum used for error-checking of the header and data. The checksum value is a hash of the data before it is sent to the receiving end. The receiving end disassembles the data packet and calculates the checksum to compare with the one it received. If the checksums don't match then the packet is dropped and a request is sent to the sender to resend the data. To ensure that the data is protected from modification during transmission; the District will utilize an SSL connection for transmission of the COR and for transfer of credentials to authenticate via the login screen. SSL protocol enables two parties to communicate with privacy and data integrity. It is the industry standard for transmitting data in a secure manner over an unsecure network. SSL provides authentication, encryption and integrity checks between the client and server communication. SSL accomplishes this by using PKI certificates. Before the data exchange happens there is an exchange of message between the client and server to authenticate each other and establish a secret key to use for encrypting any data in transmission. The same change detection methods described in item #5 is used for error checking data packets in the transmission. See attachment #17 – PKI Change Detection Process and attachment #18 – SSL Handshake Process. The exchange of documents or data will only happen through the TVE website. The website is issued a digital certificate to use for the SSL encryption. The digital certificate is issued by Network Solutions, which is a publicly recognized and trusted certificate authority. Public certificate authorities are registered to most standard browsers as trusted root certificate authorities. This means that any certificate issued by a trusted root certificate can be trusted because they have strict identity proofing processes to vouch the identity of the certificate owner. Any standard web browser should be able to navigate to the TVE website and attest to the identity or trustworthiness of it using the website's certificate. If the browser returns an error or warning about the website's certificate then the website cannot be trusted as it may not be the TVE website. This guarantees the identity of the TVE system and the user's computer during data transmission via SSL. After receiving the COR, it is archived into a secured folder that is locked down to all users except the system administrator and a special account created specifically for the TVE system to gain read-only access when processing it. District staff responsible for the review and processing of Title V reports (COR) will utilize a secured in-house application to obtain a read-only copy for reviewing purposes. Anytime a COR is requested using the in-house application, the integrity of the report is also checked automatically. Any errors or failures will be displayed on screen where the staff can then screen capture and record it into the Technical Assistance System (TAS). TAS is the District's in house software to track and record issues pertaining to technology or software systems. The District ITS team established a TAS standard for processing TAS requests so issues are resolved in a timely manner. See Attachment #22 for TAS guidelines.

System Functions:

Establishing a SSL connection between the User Client and TVE System

1. Client initiates handshake with server
2. Server responds by sending its digital certificate
3. Client verifies the server's identity by validating it against the trusted root certificate repository on its end.
4. If the identity is valid, the client generates a secret key and encrypts it with the server's public key and sends it to the server. When the server receives the secret key it decrypts it with its private key.
5. The secret key becomes the symmetric key where both client and server will use the same key to encrypt and decrypt data. The SSL connection is established at this point and is ready for transferring data.

If at any time during the data transfer via SSL an error has occurred, the client and server connection will be dropped and a new session will be established again using the process described above. If any data packets are detected to have changed then the data packet is dropped and a new data packet will be re-sent.

Also note that all errors pertaining to SSL or the website is logged on the Internet Information Services (IIS) logs. These logs are reviewed daily by the District's ITS team and any issues that are found are tracked and assigned via TAS to a support staff to investigate.

Supporting Documentation (list attachments):
Attachment #17 – PKI Change Detection Process
Attachment #18 – SSL Handshake Process
Attachment #22 – TAS Procedures and Guidelines for IT Analysts

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

9a. Notification that copy of record is available

Business Practices:
When the TVE system receives a data submittal from a user it creates a human-readable copy of it known as the COR. The COR is automatically emailed as an attachment to the user for review and offline signing. The email serves as the notification to the user that their data submittal was received and a copy of record is available for their review.

See attachments listed below for the notification email and COR samples of the ACC and RRM priority reports.

System Functions:
See system functions in item #5.

Supporting Documentation (list attachments):
Attachment #13 – Data Submittal Confirmation Email
Attachment #21a – ACC Sample Copy of Record
Attachment #22b – RRM Sample Copy of Record

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

	Business Practices: The file format specification for the initial data submittal format is a Comma Separated Value (CSV) file. See attachment #19 for the Title V electronic data standard document. When the TVE system receives the CSV formatted data it parses the data from the CSV file and uses it to create the COR consisting of all data fields described for each type of priority report (ACC or RRM) in the Title V electronic data standard document. Data is organized to accurately associate the data values with description labels. Information such as the report type, submitted by whom, date/time received and reporting periods covered are listed and clearly labeled. Larger bold fonts are used to label titles and header information. Dash lines and rectangular boxes are drawn to isolate the header from the row level data records.
	System Functions: The TVE system parses the data from the CSV file and generates a human-readable document with it. The parsed data is then recorded in the TVE database and the CSV file is retained in a secured folder for tracking and historical backup purposes. See attachments below for sample CSV files and the resulting CORs.
	Supporting Documentation (list attachments): Attachment #19 – Title V Electronic Data Standard Attachment #20a – ACC Sample Copy of Record Attachment #20b – ACC Sample CSV Data File Attachment #21a – RRM Sample Copy of Record Attachment #21b – RRM Sample CSV Data File

CROMERR System Checklist	
9c. Providing the copy of record	
	Business Practices: See item 9a.
	System Functions: See item 9a.
	Supporting Documentation (list attachments): See item 9a.
10. Procedures to address submitter/signatory repudiation of a copy of record	
	Business Practices: In the case that the user needs to repudiate the COR for any reason, they can do so via the TVE website. The process does not involve any interaction with District staff and is clearly described on the main welcome page of the website. Note that repudiation can only be performed on the COR that has not been signed by the user and submitted to the TVE system. The user should repudiate before signing and submitting the COR back and should only sign after carefully reviewing the COR and agree that it contains not errors. Optionally, the user may submit an amended data report which allows them to submit corrections to existing reports. The process to submit an amended report is the same as submitting the original. The only difference is the naming convention of the CSV data file to indicate that it is an amended data report. An amended COR will be generated and the user will still be required to review and sign it.
	System Functions: **Repudiation Process** If the user finds any reason to reject the COR then they may use the TVE website to navigate to the repudiation page and input the data ID, data type and reason(s) for the repudiation. The data ID is listed in the report header of the COR and on the data confirmation email. When the system receives a repudiation request, it will automatically flag the data records associated with the data ID provided in the request as repudiated and record the reason(s), date/time of repudiation and requested by which user. An automated email titled “Data Repudiation Confirmation” will be sent noting the data ID that was repudiated and instructing the user to resubmit new data to replace it. The new data will go through the same process as if the user is submitting it for the first time.
	Supporting Documentation (list attachments): Attachment #13 for repudiation opportunity message in the data confirmation email. Attachment #23 for the repudiation confirmation email. Attachment #24 for screen shot of TVE website link and instructions for repudiation.
11. Procedures to flag accidental submissions	

Business Practices:
Accidental submittals will be handled on a case by case basis where the user will need to contact the District directly using the contact information displayed on the contacts page of the TVE website.
The TVE website has a number of validation checks built into the submission process to prevent accidental submissions but if it does happen they will need to call the District and provide the following information to confirm the accidental submission.

- Username used in the submittal
- Filename of the data file
- Date/Time submitted

District staff will submit this information to ITS where it will be investigated to retract the accidental submittal. The user will be updated via email of the status or contacted directly if the information supplied is not sufficient to confirm the accidental submission.

System Functions:

The TVE system has a number of checks put in place to help identify accidental or erroneous submissions

Accidental Submission Preventive Steps

1. Validate all data form and field input values to make sure they conform to the expected data lengths, types, formats, and attributes.
2. Validate to make sure all required fields are present prior to acceptance and or submission.
3. Validate data filenames to make sure they conform to the format and naming convention defined under the Title V Electronic Data Standard.

Most user interface screens are built to allow the user to confirm actions such as giving them the opportunity to review data fields, files, input values, consent statements and warnings prior to submitting.

Supporting Documentation (list attachments):
N/A

CROMERR System Checklist

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

Business Practices:
The data submittal page on the TVE website has a message label added below the “Upload” button to display any error or informational messages such as letting the user know that the upload was successful.

In addition, the user is automatically emailed a data confirmation containing the COR which also serves the purpose of acknowledging the receipt of a submission.

System Functions:
Upon clicking the “Upload” button on the data submittal page to submit data the system will display a return message to a label below the button on the submission status. It will display “File uploaded. You will receive a confirmation email shortly.” for successful submissions or display an error message if there are any issues that have occurred. As indicated in the message label, an automated email will also be sent to the user as acknowledgment of a submission.

	Supporting Documentation (list attachments): Attachment #25 – Data Submittal Web Page Containing Acknowledgment Message Attachment #13 – Data Submittal Confirmation Email Containing Acknowledgment Message

CROMERR System Checklist

Signature Validation (e-signature cases only)

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

13a. Determination that credential is authentic

	Business Practices: The TVE system digital signatures are issued by the Title V Certificate Authority. This is an internal CA that issues and countersigns user digital signatures. By countersigning the user digital signatures it allows the system to later validate them for authenticity.
	System Functions: The TVE system validates the digital signature on an electronic document against the Title V Certificate Authority's digital signature to determine if the digital signature was issue by the District and that it has not expire or been revoked. If the digital signature is found to be invalid then the document will be rejected and the user will receive an e-mail informing them of the rejection and reason. See item #5 system functions section.
	Supporting Documentation (list attachments): Attachment #15 – Sample Email Message for Failed Digital Signature Validation

13b. Determination of credential ownership

	Business Practices: All user digital signatures issued by the District are protected using a password provided by the user at registration. This prevents the digital signature from being used by another person other than the user. It ensures that the owner of the digital signature provide the correct password each time the digital signature is used to sign electronic documents. Not only does the user need to provide the correct password to use the digital signature, they must also provide a valid login credential and answer a random challenge question correctly to gain access to the website in order to submit the document.
	System Functions: When the TVE system receives the submitted document it will validate the digital signature by comparing the digital signature's serial number and SHA thumb print with a data table that contains the mapping of the TVE users with their associated digital signature serials and SHA thumb prints. If the no match is found then the submission is rejected and the user will receive a rejection email with the reason. See item #5 system functions section.

	Supporting Documentation (list attachments): Attachment #6 – Digital Signature Application Screenshot (Password Field Requirement) Attachment #26 – TVE Website Login and Challenge Question Screenshot

CROMERR System Checklist	
13c. Determination that credential is not compromised	
	Business Practices: **Prevention of credential compromise** To prevent the compromise of signing credentials the District will provide the user with an application developed specifically to be used when signing electronic documents. See Attachment #6 – Digital Signature Application Screenshot. The District also requires as stated in the "Title V Digital Signature User Agreement" document that users are required to protect their digital signature and TVE account credentials by not sharing it to anyone and store them in a secured location. In addition, the transmission of signing or login credentials via the TVE website is done with a secured SSL connection to prevent anyone from intercepting and deciphering the transmission. In the event that someone repeatedly provides the wrong password for a user account 3 times in a row, the system will flag the account and lock it out for 15 minutes preventing any further login attempts. **Detection of credential compromise** To detect the compromise of signing credentials the District requires as stated in the "Title V Digital Signature User Agreement" document that all security breach pertaining to the user's digital signature must be reported to the District within 24 hours of the breach. Digital signatures on a signed document are validated against the Title V Certificate Authority to make sure they have not been modified since issued. If the signature validation fails the user will be notified via email of the failed validation. Duplicate data submissions are also detected and prevented by the TVE website. The user will get an error message if such an attempt occurs. **Rejection of known compromised credentials or submissions** In the event of a compromise digital signature, the affected credential will be immediately revoked by the District and added to the Certificate Revocation List (CRL). The CRL is a list of known digital signatures that have been revoked by the Title V Certificate Authority for whatever reason. The TVE system will reject any digital signatures that match the ones listed on the CRL.
	System Functions: See item #5.
	Supporting Documentation (list attachments): Attachment #5 – Digital Signature User Agreement Attachment #6 – Digital Signature Application Screenshot
14. Signatory authorization	
	Business Practices: The TVE System uses a number of user access control measures to determine signatory authorization and to keep user information up-to-date. Access to the TVE website signatory tools such as the digital signature download web page, Digital Signer Application and data submittal web page are only granted to those that have successfully completed the online registration process. All other users are prohibited from accessing those tools by implementation of access controls that prevent the tools from being available to unauthorized users. To ensure that user information used for authorization validation is up-to-date, the District requires as stated in the "Title V Digital Signature User Agreement" document that the user must notify the District within 5 business days if the user ceases to represent the regulated facility as signatory of

	the company's Title V report documents. This also applies if any of the user's contact information changes from what was provided at the time of registration.
	System Functions: If an unauthorized attempt is made to access the website tools then the user will be redirected to the login page. When the District receives a notification that a user is no longer authorized to sign for the regulated facility then the associated TVE account and digital signature will be deactivated and placed on the CRL. The TVE system will check the digital signature on an electronic document against the CRL list to confirm signatory authorization. When the District receives a notification to update the user's contact information, the information will be updated in the TVE database. Information that appears as part of the digital signature field attribute such as the user's full name will require revoking the current digital signature and re-issuing a new one with the updated information. All notifications are subject to verification by confirming that the notification came in through the user's registered email address or the notification was confirmed via phone by having the user verify information pertaining to their current account. In order to maintain up-to-date user information the District issued digital signatures are assigned a valid time span of 5 years from the date of issuance. Expired digital signatures are automatically revoked and will require the user to renew it by confirming or updating existing information on record. To ensure that the user have ample time to renew, an automatic email will be sent to the user when their expiration date approaches with 3 months remaining.
	Supporting Documentation (list attachments): Attachment #5 – Digital Signature User Agreement Attachment #27 – Sample Digital Signature Expiration Email Message
15. Procedures to flag spurious credential use	
	Business Practices: The TVE system is designed to identify spurious submissions and credential use using a predefined set of business rules and processes. Online data submittals are followed up by an email confirmation to the user. The user is required as stated in the Digital Signature Agreement terms that any security breach of their digital signature or TVE website account shall be immediately reported to the District within 24 hours of the occurrence. In the event that repeated attempts to login with a user account exceeds 3 times in a row, the system will flag the account and lock it out for 15 minutes preventing any further login attempts. The system tracks credential validation attempts and failures. Each morning a report of login failures is generated and reviewed by the ITS team. In addition, daily log reviews of the TVE server and associated program services are performed to identify system and security problems such as repeated failed attempts to use a credential. If any problems are found, it is immediately recorded into the TAS system where ITS will track and investigate the issue in a timely manner. The TVE system requires that the submittal data be formatted to the specifications defined in the Title V Electronic Data Standard document. The TVE system has business rules defined to validate submittal data to make sure it conforms to the standard. The validation will check for adherence to: • Filename standard • Valid data field types and sizes

	• Valid data values such as facility ID, permit number, region codes etc… Any deviation from the business rules will result in the rejection of the submission. Duplicated submissions are automatically detected during submittal and rejected with an error message screen being displayed on the web page. The system also checks signed electronic documents to make sure the required digital signatures are present and valid. See item #13 – Credential Validation
	System Functions: The system will automatically send email notifications to the user when a data submittal is rejected by the system due to a validation failure. See attachment #28 for sample email message.
	Supporting Documentation (list attachments): Attachment #5 – Digital Signature User Agreement Attachment #19 – Title V Electronic Data Standard Attachment #22 – TAS Procedures and Guidelines for IT Analysts Attachment #28 - Sample Data File Rejection Email Message

CROMERR System Checklist	
16. Procedures to revoke/reject compromised credentials	
	Business Practices: When the District is notified of a compromised credential or digital signature, the incident will be immediately entered into the TAS system for tracking and response by the ITS team. ITS will investigate and immediately lock the affected credential and or revoke the digital signature. If the digital signature was compromised then an entry is recorded into the CRL to mark the digital signature as revoked. The CRL is used during the digital signature validation process to check if a digital signature has been revoked for any reason. The affected user will need to go through the identity proofing process again to obtain new credentials or digital signature. If the TVE account was compromised then the account will be locked and assigned a secured temporary password. The user will be notified automatically by email to reset their account with the supplied temporary password. The reset process will require the user to select a new secured password.
	System Functions: The TVE system performs digital signature validation of the signed document against the CRL list to make sure signatures have not been revoked. If the validation results in a match between the CRL list and the signature on the document then the document is rejected.
	Supporting Documentation (list attachments): Attachment #29 – Certificate Revocation List (CRL) Screenshot
17. Confirmation of signature binding to document content	
	Business Practices: See Item #5 – Binding of Signature to Document Content
	System Functions: See Item #5 – Binding of Signature to Document Content

	Supporting Documentation (list attachments): See Item #5 – Binding of Signature to Document Content

CROMERR System Checklist
Copy of Record

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

18a. True and correct copy of document received

	Business Practices: The copy of record (COR) is a human-readable document generated from the data submitted. It contains digital signatures from the TVE system and the user. The digital signatures are embedded into the COR with a hash value of the document contents before each signature is applied. The digital signatures on the COR provide attestation to the identity of the parties involved and also signifies their approval of the document. The source and integrity of the COR is guaranteed with the hash value comparison of the document contents before and after signing. The original data files used to generate the COR is stored and archived in on a secured server. Chain of custody for each data file and COR is tracked by using the filename to store database index fields necessary to retrieve meta data such as when it was submitted and by which user. Additionally, the COR contains a report header that lists the same information. Resubmissions or corrections to data are allowed through amendments to the original data by way of allowing the user to resubmit the same data file containing the changes. The original data file and COR is preserved separately along with the new amended one. The user is also given an opportunity to review and repudiate the COR if they find it to be different from the original or for any other reason. If the user chooses to not repudiate and instead electronically signs the COR then it will be shown to be a true and correct copy.
	System Functions: See item #5 system functions section.
	Supporting Documentation (list attachments): Attachment #13 for repudiation opportunity message in the data confirmation email. Attachment #24 for screen shot of TVE website link and instructions for repudiation. Attachment #20a – ACC Sample Copy of Record Attachment #20b – ACC Sample CSV Data File Attachment #21a – RRM Sample Copy of Record Attachment #21b – RRM Sample CSV Data File

18b. Inclusion of electronic signatures

	Business Practices: The TVE system uses PKI digital signatures for certifying and user signing. PKI signatures are protected from being tampered with or copied to use in fraudulent signing. See item #3 and #5 for more information. The COR will have two digital signatures on it. The first signature is a certification signature by the data integrity authority. This is not the same as the certificate authority but a separate authority

	appointed by the certificate authority for the purpose of certifying the COR to guarantee the source and integrity of the document. The certification ensures that the COR does not change by locking it to prevent and control additional data being entered or appended without detection. The certification signature is applied right after the creation of the COR. Any modification to the COR after the signature will invalidate the signature. The only modification allowed after the certification is an additional signature which is the user's signature. The user signature signifies the user's approval after reviewing the COR.
	System Functions: See item #5 system functions section.
	Supporting Documentation (list attachments): Attachment #7 – District's PKI Infrastructure Diagram Attachment #8 - X509 Digital Signature Field Specification Attachment #11 – PKI Whitepaper Attachment #12 – PKI Infrastructure Abstract
18c. Inclusion of date and time of receipt	
	Business Practices: The timestamp of when the report was received is visible as the "Received Date" text field in the COR. When report data is received through an online submittal the TVE system generates a COR using the data and digitally signs it to certify the document. This process binds the receive date and time to the document.
	System Functions: When the TVE system receives an online data submittal it records the date and time of when the data was received. The date and time is later added to the COR during the creation process.
	Supporting Documentation (list attachments): Attachment #14 – Sample Certified and Signed COR Document

CROMERR System Checklist	
18d. Inclusion of other information necessary to record meaning of document	
	Business Practices: The COR includes other information such as the Report Type, Facility Name, Facility ID, Data ID, Reporting Period, and Submitted By fields. These fields are clearly labeled at the top of each page to help identify the contents and meaning of the associated COR document. In addition, there is a visible digital signature widget for each signature that is applied to the COR. The certification signature widget is located on the top left hand corner of the first page and the user signature widget is located on the last page in a box labeled "Digital Signature of Responsible Official". The widgets bear the District's logo and are clickable to display the digital signature's property information.
	System Functions: When the TVE system receives an online data submittal it parses the data file name for index values that identifies the report type, submitting facility, reporting period of the data and makes a data entry record to track the index fields. These index fields are later used to populate the report header of the COR used to identify the document and its contents. There is a clickable widget added to the designated area of the COR when a signature is applied. See attachment #14 to view the additional information fields and signature widgets.
	Supporting Documentation (list attachments): Attachment #14 – Sample Certified and Signed COR Document
18e. Ability to be viewed in human-readable format	
	Business Practices: In addition to the other information listed in item #18d, the COR contains the data field values organized into data rows and columns that are clearly labeled. Formatting such as underlining columns and using broken line bars to distinguish between different rows are used to help make it easy to read the data. All COR documents will be provided in the PDF file format.
	System Functions: The TVE system requires the initial data submittal to be in a CSV format for system automation purposes. A CSV file is not human readable so after validating the data within the file, the system transforms the data into the COR. The transformation process will put the data into a human-readable format consisting of descriptive data labels, report header on each page, and use of row level reporting. The file type used to save the COR is a PDF type, which is supported by many types of document viewing software available. It is recommended that the readily available and free Adobe Reader Software be used to view the PDF document. The COR is automatically emailed as an attachment to the user for viewing and review before electronically signing it.
	Supporting Documentation (list attachments): Attachment #14 – Sample Certified and Signed COR Document
19. Timely availability of copy of record as needed	

	Business Practices: The TVE system retains all information and data used to generate the COR on a secured server in addition to archiving the COR into the District's Electronic Document Management System (EDMS). The COR is archived unmodified with all electronic signatures on it. It is indexed by the facility ID, report type, and document date so that it can be queried and retrieved quickly when needed. The COR can be provided through the Public Records Release Request (PRR) process. Generally, the District has up to 10 days to respond to the requester if the data requests is feasible and a time estimate which may include applicable processing fees. Time estimate may vary depending on the type of data request but for 1 COR request to serve litigation purposes, it is feasible to assemble the data within 1 business day. The assembled data would include an electronic CD-ROM disc containing: • COR document • CSV data file (Original submitted data used to generate the COR) • Information such as the date/time the data was submitted, by whom, who the signatories were and what they certified. • Information to demonstrate the digital signature chain showing that the District CA is the issuer of the digital signatures (Data Certification and User Signature) present on the COR. Information on requesting a PRR is available on the District's website at www.valleyair.org. Also note that the District currently does not have a document retention policy in place so all CORs will remain in EDMS indefinitely at this time.
	System Functions: N/A
	Supporting Documentation (list attachments): Attachment #31 – Public Records Release Request Web Page Screenshot Attachment #32 – Public Records Release Guidelines

CROMERR System Checklist	
20. Maintenance of copy of record	
	Business Practices: COR documents are stored on secured EDMS servers where only the system administrator has direct full access to the documents in the event that such access is necessary to troubleshoot an issue. These documents are stored in a read-only state. Daily tape backups of the documents are performed on a nightly basis. The documents are also replicated to two additional servers for document access and redundancy purposes. In the event of a data failure, the document can be restored from tape backup or from any of the two replicated servers. Daily server log reviews are performed to identify security or system related issues with the servers and documents stored on them. There is also an EDMS replication audit report that shows the integrity of the number documents stored in all three servers to ensure that they are all identical in terms of document storage.
	System Functions: There are a total of three EDMS servers that are synchronized and backed up on a nightly basis. Each morning a process prints out two reports that summarize the replication status and the status of the system. See attachments.
	Supporting Documentation (list attachments): Attachment #33 – EDMS Replication Report Attachment #34 – EDMS NT Event Log Report