|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Item** |  |
| **Registration (e-signature cases only)** | |
| **1. Identity-proofing of registrant** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **1a. (priority reports only) Identity-proofing *before* accepting e-signatures** | |
|  | **Business Practices:** |
| **System Functions:** |
| **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:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **1bii. (priority reports only) Information or objects of independent origin** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **1b-alt. (priority reports only) Subscriber agreement alternative** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **2. Determination of registrant's signing authority** | |
|  | **Business Practices:**  **[Insert business practices for State, Local, or Tribal agency]**  CAERS Determination of Signing Authority for Reporting Facilities:  CAERS Business Process  The core CAERS business process is the submission of an annual emissions report from reporting facilities to **[Insert State, Local, or Tribal agency name]**, who reviews the report before submitting to the EPA National Emissions Inventory and current and future downstream systems using data and reports submitted to CAER, such as the eGRRT system. **[Insert State, Local, or Tribal agency name]** representatives work directly with facility representatives from their jurisdictions to support and govern their emissions reporting. In the CAERS system, a **[Insert State, Local, or Tribal agency name]** CAERS Reviewer may authorize or remove authorization for registered regulated community reporters to view, enter, submit, and certify emissions reports for specific facilities in their jurisdiction.  **[Insert State, Local, or Tribal agency name]** Onboarding  When **[Insert State, Local, or Tribal agency name]** begins using the CAERS system for accepting annual emissions reports they will work with the CAERS Program Office (PO) to initiate the onboarding process. The EPA Central Data Exchange (CDX) Change Control Board (CCB) will be notified when **[Insert State, Local, or Tribal agency name]** begins the onboarding process for CAERS. As part of the onboarding process, **[Insert State, Local, or Tribal agency name]** will complete this CDX CROMERR checklist where they describe in detail their process for determining a user’s signing authority for a facility in their jurisdiction. **[Insert State, Local, or Tribal agency name]** will submit the CROMERR checklist for approval by the CDX CROMERR team. **[Insert State, Local, or Tribal agency name]** will also submit a completed CROMERR application cover sheet and satisfy CROMERR legal certification requirements.  No **[Insert State, Local, or Tribal agency name]** facilities or **[Insert State, Local, or Tribal agency name]** SLT Reviewers will be onboarded to CAERS in CDX production until the **[Insert State, Local, or Tribal agency name]** CROMERR package has been approved and the Federal Register notice of approval is published.  Access to SLT Reviewer role in CAERS  Once the **[Insert State, Local, or Tribal agency name]** onboarding process is complete, individuals who are to receive the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer role in CAERS will register with an account in CDX. Once registered, the CAERS PO will request that the CDX Help Desk grant the user the “SLT Reviewer” role in the CAERS dataflow along with the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer for which they are authorized to represent, which is a closed registration.  The CAERS system will make available electronically the “CAERS SLT Reviewer Rules of Behavior” (see Attachment 1) to the individuals for their review and signature. Once the user has electronically signed the Rules of Behavior, the Help Desk will grant the user the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer role in CAERS dataflow and specify the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer that this user is allowed to administer. The user can now log into CDX, choose the SLT Reviewer role. CAERS allows **[Insert State, Local, or Tribal agency name]** CAERS Reviewers to accept and reject emissions reports for facilities in their jurisdiction, manage information for their facilities, transmit accepted emissions reports to the EIS, etc. **[Insert State, Local, or Tribal agency name]** CAERS Reviewers can also authorize and remove authorization in CAERS for regulated community Certifiers to facilities in their jurisdiction.  Process for Certifier Users to request signing authorization for a facility in CAERS  A Certifier user registers in CDX following the standard registration procedures described in the EPA CAER CROMERR Application Checklist section 1. A user who wishes to be granted signing authority for a facility in CAERS must register for the Certifier role, and successfully complete the identity proofing process, and electronic signature agreement process as described in the EPA CAER CROMERR Application Checklist section 1. At this point they can access the CAERS but cannot view any data or any emissions reports for any facilities. The **[Insert State, Local, or Tribal agency name]** CAERS Reviewer must explicitly grant authorization to individuals registered in CDX with the Certifier roles to allow them to view, enter, submit, and certify data reports for facilities in **[Insert State, Local, or Tribal agency name]**’s jurisdiction. Certifier users have no Read, Write, or Item 2 Signing/Certification “Authority” at this point.  The Certifier user:  1. Selects the “Request Access to a New facility” button on the “My Facilities” screen  2. Searches for a facility specifying the SLT of the facility and other search criteria (Facility Name, SLT Facility ID, etc.)  3. Selects the Facility from the returned list that matches their criteria and selects the “Request Access” button.  An email notification is sent to the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer at the email address specified on the SLT reviewer properties alerting them that a user has requested access to a facility, and including the username, the facility name, the facility id, and the CAERS role being requested (Certifier or Preparer). The **[Insert State, Local, or Tribal agency name]** CAERS Reviewer can log into CAERS, view authorization requests on the “Pending Authorization Requests” screen.  At this point, the **[Insert State, Local, or Tribal agency name]** CAERS Reviewers follow the processes described in this CROMERR application package and in compliance with the signed rules of behavior to validate the user’s signing authority for the requested facility. Once the signing authority has been determined, the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer can log into the CAERS system and either approve or reject the request on the “Pending Authorization Requests” screen. According to the Rules of Behavior that **[Insert State, Local, or Tribal agency name]** CAERS Reviewers will sign, **[Insert State, Local, or Tribal agency name]** will perform determination of the registrant's signing authority as described in this CROMERR application.  When the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer indicates that they wish to approve the request in CAERS a modal dialogue provides the following language. “I acknowledge that by clicking ‘Proceed’ I am authorizing these individuals to prepare and/or submit reports for the requested facilities. I have verified the individuals’ signing authority for these facilities according to the process described in the CAERS onboarding documentation for my SLT.” The **[Insert State, Local, or Tribal agency name]** CAERS Reviewer will click “Proceed” or “Cancel” to either proceed with the authorization or cancel. The **[Insert State, Local, or Tribal agency name]** CAERS Reviewer also has the option to “Reject” the authorization request and provide a “Reason for Rejection” to the requestor via an automated email.  An email notification will be sent to the Certifier CAERS registrant with details of the approval or rejection with a CC to the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer. Once approved, a Certifier user can log into CAERS and access the facility and its emissions reports from the My Facilities screen.  Deauthorization  **[Insert State, Local, or Tribal agency name]** will follow the processes described in this CROMERR application package and also the signed CAERS Rules and Behaviors for SLT Reviewers in order to determine when a user is no longer associated with a facility in their jurisdiction. This involves a notice from the facility representatives that a given individual is no longer a valid representative for their facility. The **[Insert State, Local, or Tribal agency name]** CAERS Reviewer can navigate to the Facility Information page in CAERS, view the users authorized for the facility and remove their authorization. If the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer is notified that an authorized Preparer or Certifier has left the company or otherwise no longer has signature authorization for an entity, **[Insert State, Local, or Tribal agency name]** must contact CDX help desk and inform them.  Retaining Information on Authorizations and Deauthorizations  The following information is recorded in the CAERS database ACL tables to record the authorization:   1. The CDX Role ID making the request (User account + Role). 2. The CAERS facility record id the user is being authorized for. 3. The CDX user id of the SLT official who authorized the access. 4. The full name of the SLT official who authorized the access. 5. The timestamp when the user was authorized for the facility.   Record of this information will be maintained by CDX with stated information for 5 years after signature device is revoked or rejected.  **[Insert State, Local, or Tribal agency name]** can at any time remove the authorization of a user to report for a facility. When the **[Insert State, Local, or Tribal agency name]** CAERS Reviewers click the Delete button on the Facility Information screen to remove a user the ACL table described above is updated to add the timestamp when the authorization was removed and the **[Insert State, Local, or Tribal agency name]** CAERS Reviewer who removed the authorization. This maintains an ongoing record of all authorizations over time when any user had authorization to report for a facility. |
| **System Functions:**   * Registrant submits a request to be a Certifier for a specific facility in CAERS, which must be approved by a state Reviewer. * **[Insert State, Local, or Tribal agency name]** staff reviews Certifier request and verifies signing authority prior to granting the request.   During the CDX User Registration or Profile Update processes, the CDX system provides the necessary instructions/forms and prompts the prospective user to complete and mail evidence of signatory authorization to the PO or CDX Help Desk or provides the link to LexisNexis verification of organizational affiliation. These steps are performed through a series of web-based dialog screens.  CDX employs an application role-based authorization system. By default, the creation of a CDX account does not grant the user any rights or privileges for e-signature or Public Key Infrastructure (PKI) applications, thus prohibiting them from making signed data submissions until the processes of identity-proofing and determination of authorization are completed.  The CDX system provides a web-based mechanism (called Registration Maintenance) for a delegated CDX user registration authority (known as RMAMs) or the CDX Help Desk to grant, deny, or revoke application access to prospective users after determination of the user’s signatory authority (see Attachment 3 from the EPA CAER CROMERR Application). This authorization action (and the ID of the authorizing RMAM) is recorded by the CDX system and an approval/disapproval notification sent to the prospective user and other associated RMAMs. Access to the Registration Maintenance function is strictly controlled through the use of user ID/password credentials. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **3. Issuance (or registration) of a signing credential in a way that protects it from compromise** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **4. Electronic signature agreement** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Signature Process (e-signature cases only)** | |
| **5. Binding of signatures to document content** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **6. Opportunity to review document content** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **7. Opportunity to review certification statements and warnings** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Submission Process** | |
| **8. Transmission error checking and documentation** | |
|  | **Business Practices:** |
| **System Functions:** |
| **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:** |
| **Supporting Documentation (list attachments):** |
| **9b. Creation of copy of record in a human-readable format** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **9c. Providing the copy of record** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **10. Procedures to address submitter/signatory repudiation of a copy of record** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **11. Procedures to flag accidental submissions** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **12. (e-signature cases only) Automatic acknowledgment of submission** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Signature Validation (e-signature cases only)** | |
| **13. Credential validation (See 13a through 13c)** | |
| **13a. Determination that credential is authentic** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **13b. Determination of credential ownership** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **13c. Determination that credential is not compromised** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **14. Signatory authorization** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **15. Procedures to flag spurious credential use** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **16. Procedures to revoke/reject compromised credentials** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **17. Confirmation of signature binding to document content** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **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:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **18b. Inclusion of electronic signatures** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **18c. Inclusion of date and time of receipt** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **18d. Inclusion of other information necessary to record meaning of document** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **18e. Ability to be viewed in human-readable format** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |
| **19. Timely availability of copy of record as needed** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **20. Maintenance of copy of record** | |
|  | **Business Practices:** |
| **System Functions:** |
| **Supporting Documentation (list attachments):** |