INTRODUCTION: BACKGROUND TO CROMERR

Welcome to Cross-Media Electronic Reporting Regulation (CROMERR) 101: Fundamentals for States, Tribes, and Local Governments.

This course is designed for states, tribes, and local governments who:

- Administer EPA-authorized programs under Title 40 of the Code of Federal Regulations (40 CFR); and
- Accept or wish to accept electronic reports.

The course consists of eight lessons.

Throughout the course, you will encounter certain words and phrases that appear as blue, underlined, hyperlinked text. These are key terms that have specific meaning. By selecting the blue words, which are hyperlinks, the CROMERR definition of that term will appear in a pop up box.

In addition, print icons are provided in the top right-hand corner of each page. By selecting these icons, you may print the entire content of each page, even if that content is minimized or hidden. If you are accessing this training with a screen reader, you may print all content on each page by using the browser's normal print functionality.

Also, back and next links are provided to the right above and below all page content to allow quick navigation through the course pages. On pages where course content is particularly substantive, these back and next links will instead move you through important sub-points.Please note that this training does not apply to direct reporters. If you report directly to EPA, please refer to the section on CDX at the end of this document.

States—For purposes of CROMERR, the term “states” includes the District of Columbia and the United States Territories, as specified in the applicable statutes.

EPA-Authorized Programs—States, tribes, and local governments that have been delegated, authorized, or approved, or that seek delegation, authorization, or approval to administer a federal environmental program under Title 40 of the Code of Federal Regulations (CFR).

Title 40—The Code of Federal Regulations (CFR) is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the federal government. The CFR is divided into 50 sections, called “titles.” Title 40 is the section of the CFR that deals with EPA’s mission to protect human health and the environment.

WHAT IS CROMERR?

CROMERR provides the legal framework for electronic reporting from regulated entities to the Environmental Protection Agency (EPA) and to states, tribes, and local governments that are authorized to administer EPA programs.

The intent of CROMERR is to maintain the same level of corporate and individual responsibility and accountability that exists in the paper environment when reporting is done electronically. CROMERR supports many of the benefits of electronic reporting, including:

- Allowing government agencies and regulated entities to interact electronically;
- Fostering more rapid and accurate environmental reporting and posting of compliance information;
- Simplifying facility reporting processes;
- Making data more readily available; and
- Maintaining consistency with emerging industry practices.

THE CROMERR TIMELINE

CROMERR was codified in the Code of Federal Regulations (CFR), Title 40, Part 3 on October 13, 2005. It was then amended on December 24, 2008 to extend compliance dates for existing systems.

Under this amendment, programs with an existing e-reporting system were required to submit an application for EPA approval no later than January 13, 2010. This is an extension from the original deadline of October 13, 2007.

New e-reporting systems are also required to submit an application for EPA approval prior to receiving e-reports.

Existing Systems: An existing electronic document receiving system is one that:

- Received e-documents, in lieu of paper, on or before October 13, 2005; or
- Was substantially developed on or before October 13, 2005, as evidenced by the establishment of system services or specifications by contract or other binding agreement.

REGULATED ENTITIES REPORTING DIRECTLY TO EPA

Under CROMERR, electronic reporting directly to EPA requires submission through EPA's Central Data Exchange (CDX), or to another system designated by the EPA Administrator for the receipt of the electronic report in question. Following the procedures established by CDX for document preparation, signature, and submission ensures submitted documents are not only successfully received by CDX, but also comply with CROMERR.

Note that submissions must include valid electronic signatures in those cases where handwritten signatures would have been required for the paper-base submissions, and the electronic signatures will have the same legal force as the handwritten signatures.

Valid electronic signatures: Valid electronic signature refers to an electronic signature on an electronic document that has been created with an electronic signature device.

The identified signatory is uniquely entitled to use the signature device for signing that document provided that this device has not been compromised, and where the signatory is an individual who is authorized to sign the document by virtue of his or her legal status or his or her relationship to the entity on whose behalf the signature is executed.

THE CENTRAL DATA EXCHANGE (CDX)

The CDX enables fast, efficient and more accurate environmental data submissions from states, tribes, local governments, and industry to EPA and participating program offices.

EPA's CDX is the point of entry on the Environmental Information Exchange Network (Exchange Network) for environmental data submissions to the Agency. CDX works with both EPA program offices looking for a way to better manage incoming data, and stakeholders looking for a way to reduce time and money spent to meet EPA reporting requirements. CDX provides stakeholders with the ability to:

- Submit data through one centralized point of access;
- Fill out a single electronic form that can be submitted instantaneously instead of mailing multiple paper forms;
- Receive Agency confirmation when submissions are received;
- Submit data in a variety of formats including Webs Forms, XML, binary, or flat-file;
- Exchange data with target systems using Web services;
- Reduce costs associated with submitting and processing data submissions;
- Utilize publishing services to share information collected by EPA with other stakeholders, including states and tribes.

Information on the submissions that CDX currently accepts can be found on the CDX website. Whenever CDX or another EPA-designated system is ready to accept additional electronic submissions, EPA will publish an announcement in the Federal Register, and will provide information with the procedures for electronic submission of the affected reports. For submissions that CDX accepts, the CDX website will provide instructions concerning the format required for data submission, registration procedures, and requirements for electronic signatures.

LESSON 1: OVERVIEW OF THE FINAL RULE

This lesson provides an overview of CROMERR, as codified in the CFR.

Topics covered in this lesson include:

- What does the rule do?
- What does the rule NOT do?
- Who is affected?
- When does the rule NOT apply? (Or "What are the exceptions to the rule?")
- What are the compliance dates?

WHAT DOES THE RULE DO?

- Sets Standards for e-Reporting: The rule sets standards for systems that states, tribes, and local governments use to receive e-reports under their EPA-authorized programs. The standards are performance-based requirements that systems must meet to ensure the authenticity and integrity of the electronic documents and electronic signatures that they receive. EPA systems that receive e-reports from direct reporters are also required to meet these CROMERR standards.
- Removes Regulatory Obstacles: The rule removes regulatory obstacles to e-reporting under EPA and EPA-authorized programs by overriding references to paper-based requirements in Title 40 of the CFR. Examples include "file copies" or "return receipts."

Sets Requirements for:

- Direct e-Reporting to EPA: The rule sets requirements for regulated entities that report directly to EPA and wish to report electronically. The requirements identify the EPA systems to which they may e-report and set conditions on the execution of any signatures associated with the submitted reports.
- Authorized Programs That Receive or Wish to Receive e-Reports: The rule requires state, tribal, and local governments that receive or wish to receive e-reports in lieu of paper under their authorized programs to seek EPA approval of modifications or revisions to those programs to incorporate e-reporting. EPA will make approval decisions based primarily on two criteria:
  - The applicant must have sufficient legal authority to enforce its authorized programs using electronically submitted documents; and
  - The system the applicant proposes to use to receive the e-reports must meet the CROMERR standards for e-reporting systems.

These criteria reflect the need to ensure that the applicant preserves the enforceability of its authorized programs when replacing paper reports with e-reports.

- Applications for EPA Approval of Authorized Program e-Reporting: The rule sets requirements for completing and submitting an application for approval of an authorized program modification or revision, including a specification of the items that the application must include.

And:

- Provides a Special, Streamlined EPA Approval Process: CROMERR provides a streamlined approval process for program modifications or revisions related to e-reporting that allows state, tribal, and local governments to submit a single, consolidated application for multiple authorized programs. State, tribal, and local governments may also use applicable program approval or revision processes under other Parts of Title 40 that are specific to a particular authorized program.

WHAT DOES THE RULE NOT DO?

- Does NOT Set Requirements for e-Recordkeeping: The rule does NOT set requirements for regulated entities that maintain records required under EPA and EPA-authorized programs that wish to maintain those records electronically.
- Does NOT Make e-Reporting Mandatory: CROMERR does NOT mandate that authorized programs institute electronic reporting or accept documents electronically. It also does NOT require that regulated entities use electronic reporting to report directly to EPA.
- Does NOT Prohibit Mandatory e-Reporting: CROMERR does NOT prohibit mandatory e-reporting under other federal, state, tribal, or local laws.

WHO IS AFFECTED?

The final rule applies to two groups:

- **Regulated Entities—**CROMERR applies to persons or entities that submit electronic reports or documents in lieu of paper, to EPA under Title 40 when they are the regulated entity.
  - For example, 40 CFR 51.211 requires that operators of stationary sources of air emissions, such as power plants, must periodically report those emissions. If a regulated entity submits this report electronically directly to EPA, it is subject to CROMERR.
- **Entities Acting as a Regulator for an EPA Program—**States, tribes, or local governments that administer authorized programs under Title 40 that receive or wish to receive electronic reports or documents in lieu of paper.
  - The Clean Water Act (CWA) Program is an example of how states, tribes, or local governments can act as a regulator for an EPA program. The CWA gives EPA the authority to set effluent limits on an industry-wide (technology-based) basis and on a water-quality basis. These limits will ensure protection of the receiving water. The CWA requires anyone who wants to discharge pollutants to first obtain a National Pollutant Discharge Elimination System (NPDES) permit.

- The CWA allows EPA to authorize the NPDES Permit Program to state governments, enabling states to perform many of the permitting, administrative, and enforcement aspects of the NPDES Program.

In lieu of paper: An electronic report is considered to be submitted "in lieu of paper" when it takes the place of a paper report submitted to satisfy the requirements under another part of 40 CFR.

In some states, the electronic reporting is done to make data collection and management easier, but the state requires that each report submitted electronically also be submitted as a signed paper copy. In this case, the electronic submission would not be in lieu of paper and CROMERR does not apply to the state.

Some electronic reporting systems use a combined approach, where part or all of the data are submitted only electronically, but a wet ink signature on paper is also required. In these cases, the e-report (or at least the portions of it that are not also submitted on paper) is considered to be submitted "in lieu of paper" and CROMERR applies.

In addition, there are special CROMERR rules under 40 CFR 3.2000(a) that govern the use of a wet ink signature on paper in conjunction with an e-report. (Additional detail on this combined approach is provided in Lesson 6.)

When Does the Rule NOT Apply?

CROMERR does **NOT** apply to:

1. Documents submitted via fax, or magnetic or optical media, including:
   - Facsimile transmissions;
   - Tape;
   - Diskette;
   - Compact Disc (CD); and
   - Digital Video Disc (DVD).
2. Data transfers between EPA and state, tribal, or local governments when the transfers are:
   - Part of their authorized programs; or
   - Part of administrative arrangements with EPA.
3. Submissions to EPA not under Title 40
4. Submissions to state, tribal, or local governments not under their authorized programs

WHAT ARE THE COMPLIANCE DATES FOR STATES, TRIBES, AND LOCAL GOVERNMENTS' AUTHORIZED PROGRAMS?

Authorized programs must meet CROMERR's compliance dates:

- New e-Reporting Systems: Programs with a new e-reporting system, as defined in CROMERR, must seek EPA approval ***before*** using that system to receive e-reports in lieu of paper.
- Existing e-Reporting Systems: Programs with an existing e-reporting system were required to submit an application for EPA approval no later than January 13, 2010.

Note: The requirement was for programs to submit the application by this deadline; the program need not receive EPA approval by that deadline. The program may continue to operate the existing e-reporting system while the application is under review.

LESSON 2: QUICK TOUR OF THE FINAL RULE

This lesson provides an introduction to how the rule is structured, the subparts of the rule, and what each subpart contains.

ADDITIONAL RESOURCES:

- CROMERR Federal Register Notice Preamble and Regulation (PDF);
- CROMERR Concurrent Federal Register Notice (PDF); and
- CROMERR Final Rule (PDF).

SUBPART A: GENERAL PROVISIONS

Subpart A answers the following questions:

TO WHOM DOES THIS PART APPLY?

This section provides a description of the persons and entities impacted by the rule.

HOW DOES THIS PART PROVIDE FOR ELECTRONIC REPORTING?

Subpart A describes how the regulation makes provision for electronic reporting.

WHAT DEFINITIONS ARE APPLICABLE TO THIS PART?

Many terms used throughout the rule have very specific definitions in regard to the rule and are therefore defined in Section 3.3 of the CROMERR Regulation.

HOW DOES THIS PART AFFECT THE ENFORCEMENT AND COMPLIANCE PROVISIONS OF TITLE 40?

This section describes how the rule relates to compliance with Title 40 and the enforcement provisions therein.

SUBPART B: ELECTRONIC REPORTING TO EPA

Subpart B answers the following questions:

WHAT ARE THE REQUIREMENTS FOR ELECTRONIC REPORTING TO EPA?

Subpart B describes when e-reporting can be used and under what circumstances.

HOW WILL EPA PROVIDE NOTICE OF CHANGES TO THE CENTRAL DATA EXCHANGE (CDX)?

Subpart B also describes how and when EPA will provide notification of changes to hardware and software associated with the CDX that may impact electronic transmission.

SUBPART C HAS BEEN INTENTIONALLY LEFT BLANK FOR NOW. IT IS RESERVED FOR ELECTRONIC RECORDKEEPING PROVISIONS, WHICH HAVE NOT YET BEEN FINALIZED.

Subpart D: Electronic Reporting Under EPA-Authorized State, Tribal, and Local Programs

Subpart D contains the majority of the CROMERR requirements and answers the following questions:

How do states, tribes, or local governments revise or modify an authorized program to allow electronic reporting?

Subpart D describes what is necessary in order to conduct e-reporting, including the processes for application and EPA approval.

What are the requirements that authorized states, tribes, and local programs' electronic report receiving systems must meet?

This subpart provides a detailed listing of the requirements that must be met in order to have a CROMERR-compliant system.

Central Data Exchange (CDX) refers to EPA's centralized electronic document receiving system, or its successors, including associated instructions for submitting electronic documents. More information on the CDX is available in the "Helpful Resources" section of this training, accessible through the main menu.

LESSON 3: APPLICATION REQUIREMENTS

This lesson is for states that plan to submit CROMERR applications to EPA to modify or revise their authorized programs to incorporate electronic reporting. This lesson includes details about the application as well as instructions for submission. The result of EPA approval is to modify or revise those programs.

This lesson covers:

- Required elements of a CROMERR application;
- Typical application components used to meet the requirements; and
- Submitting the application.

These topics are covered from the perspective of states using the CROMERR Part 3 Application Process. States may apply for their program revisions or modifications using processes provided under other parts of Title 40, but their applications must still include the same required elements described in this lesson.

WHAT EXACTLY ARE YOU SUBMITTING THE APPLICATION FOR? WHAT IS REQUIRED FOR APPLICATION APPROVAL?

The application submitted to EPA is for approval of modifications or revisions to allow electronic reporting for one or more of the EPA-authorized programs implemented by your state. That is, you are seeking EPA approval to allow you to accept electronic documents in lieu of paper for submissions made by facilities regulated under your state's authorized programs. For EPA to approve the program modifications, your state attorney general, or AG, must be able to certify that the state can continue to enforce these authorized programs based on electronic submissions. In addition, the system used to receive the electronic submissions must meet the standards spelled out in Section 3.2000 of CROMERR. These standards are discussed in detail in Lessons 5, 6, and 7 of this course.

USING PROCESSES PROVIDED UNDER OTHER PARTS OF TITLE 40

There are two ways to submit a CROMERR application. This lesson is focused on the special 40 CFR Part 3 Application Process, but applications may also be submitted under other parts of Title 40.

Applications submitted to EPA Program or Regional Offices under other parts of Title 40 must:

- Use applicable program approval or revision processes under other Parts of Title 40;
- Meet the application requirements under § 3.1000; and
- Demonstrate conformance with § 3.2000 requirements.

Regardless of the process used, the required application elements are the same. However, non-Part 3 applications can only address a single program.

REQUIRED ELEMENTS OF A CROMERR APPLICATION

Under § 3.1000(b)(1), to obtain EPA approval of program revisions or modifications to incorporate electronic reporting, a state, tribe, or local government must submit an application to the EPA Administrator that includes the four elements below.

- AG Certification—The AG Certification demonstrates that the state has sufficient legal authority to enforce the program using electronic reports as described in §3.2000(c).
  - §3.1000(b)(1)(i) A certification that the state, tribe, or local government has sufficient legal authority provided by lawfully enacted or promulgated statutes, or regulations that are in full force and effect on the date of the certification, to implement the electronic reporting component of its authorized programs covered by the application in conformance with §3.2000 and to enforce the affected programs using electronic documents collected under these programs—together with copies of the relevant statutes and regulations, signed by the state AG, their designee, or, in the case of an authorized tribe or local government program, by the chief executive or administrative official or officer, also known as the CAO, of the governmental entity, or their designee.
- System Descriptions—The System Description(s) section demonstrates that systems used to receive e-reports meet the CROMERR standards listed in §3.2000(b), and provide for e-signatures (or follow-on paper signatures) that meet the requirements of §3.2000(a).
  - (ii) A listing of all the state, tribe, or local government electronic document receiving systems that will accept the electronic documents addressed by the program revisions or modifications covered by the application, together with a description for each such system that specifies how the system meets the applicable requirements in §3.2000 with respect to those electronic documents.
- System Upgades—The System Upgrades section identifies any system changes that may affect CROMERR compliance.
  - (iii) A schedule of upgrades for the electronic document receiving systems listed under paragraph (b)(1)(ii) of this section that have the potential to affect the program's continued conformance with §3.2000.
- Other Information—The Other Information section provides additional information that should be considered by EPA during evaluation of the application.
  - (iv) Other information that the EPA Administrator may request to fully evaluate the application.

A note about non-Part 3 applications—These requirements are applicable for Part 3 and Non-Part 3 Applications. However, remember that Non-Part 3 Applications can generally address only one program.

TYPICAL APPLICATION COMPONENTS

Typical CROMERR applications include a minimum of three components, which are listed below. The first component, the Cover Sheet, is not listed on the previous page as a required element; however, it represents a best practice for organizing basic application information. The other two application components directly reflect CROMERR-required elements.

- The Cover Sheet captures basic contact and program information and identifies the programs to be modified or revised by EPA approval of the application, along with the associated reports and systems.
- As previously described, the AG Certification demonstrates that the state has sufficient legal authority to enforce the program using e-reports as described in § 3.2000(c).
- The System Description(s) component demonstrates that systems used to receive e-reports meet the CROMERR standards included in § 3.2000(b), and provide for e-signatures (or follow-on paper signatures) that meet the requirements of § 3.2000(a). This component also documents any anticipated system upgrades that will affect conformance with the CROMERR standards.

These application components are described in greater detail in the following pages.

Note that EPA offers a number of tools and templates to help states develop these application components. These tools and templates are described in greater detail in later lessons.

COVER SHEET

The Cover Sheet documents basic information about who is submitting the application and what they are applying for.

Although the Cover Sheet format is not required, EPA needs the information on the Cover Sheet in order to process your application. For example, program citations for reports addressed by your state's application are requested to ensure that EPA approval actually modifies or revises the programs to cover the electronic reporting you want to implement.

The Cover Sheet includes data fields for:

- Type of agency;
- Application point of contact;
- List of components included in this CROMERR application;
- Brief system overview;
- List of programs covered by the application; and,
- List of attachments included with the application.

RELATED RESOURCES:

- Blank Cover Sheet (PDF) (3 pp. 219 K)

ATTORNEY GENERAL (AG) CERTIFICATION

The AG Certification is a letter confirming legal authority to implement the electronic reporting covered by the application and enforce the affected programs using the electronic documents received under those programs.

- For states, the AG, or his or her designee, must sign the certification letter.
- For tribes and local governments, the chief administrative official or officer (CAO), or his or her designee, must sign the certification letter.
- In either case, letters signed by a designee must explicitly state that this individual has delegated authority from the AG (or CAO) to sign the certification letter.

The certification must include copies of all state, tribal, or local statutes and regulations relevant to the application. EPA suggests also including a description specifically linking applicable portions of 40 CFR Part 3 to relevant portions of the state, tribe, or locality's statutes and regulations to facilitate EPA's review.

RESOURCES:

- CROMERR Legal Certification Guide for State Attorney General or Local Government or Tribe Certifying Official Statement (PDF) (13 pg, 198K)

SYSTEM DESCRIPTION(S)

The System Description component documents how the system(s) meet the CROMERR standards.

To help applicants complete this description, EPA has developed a CROMERR System Checklist Template and strongly encourages you to use it. The template reflects the Checklist Requirements Roadmap, which lays out the CROMERR standards as a list of 20 performance-based system requirements. These requirements are divided into five categories: Registration, Signature Process, Submission Process, Signature Validation, and Creation of the Copy of Record (COR).

The descriptions that an applicant provides for each of the 20 checklist requirements reflect how the applicant's system(s) will meet the CROMERR standards. When applicable, supporting documentation should be attached to the descriptions. Such attachments may include the Electronic Signature Agreement, system users' guides, various process diagrams, and system screenshots and/or printouts. The CROMERR standards are explained in Lesson 6. Lesson 7 then describes how the CROMERR standards are expressed as checklist requirements, and explains how to use the System Checklist Template.

RESOURCES:

- Blank System Checklist (DOC) (13 pp, 60 K);
- CROMERR System Checklist (XLS) (71 K); and
- Sample Approved Delaware CROMERR System Checklist (PDF) (35 pp, 1017 K).

SUBMITTING THE APPLICATION

Applications submitted using the 40 CFR Part 3 approval process must be sent to the attention of EPA's Office of Environmental Information.

The majority of application materials can be submitted electronically by e-mailing these materials to the CROMERR Program general mailbox (cromerr@epa.gov) and Karen Seeh (seeh.karen@epa.gov). Hard-copy application file submissions are no longer required. If attempting to send application files larger than 8 MB, please contact us to arrange for transfer.

The attorney general certification is the only application document that still must be sent in hard copy. This document can be sent directly to the attention of Karen Seeh at one of the addresses below.

- For U.S. Postal Service deliveries: 1200 Pennsylvania Avenue, NW, Mail Code 2823T, Washington, DC, 20460
- For UPS, FedEX, or courier mail deliveries: 1301 Constitution Avenue, NW, EPA West, Room 6408J, Washington, DC, 20004

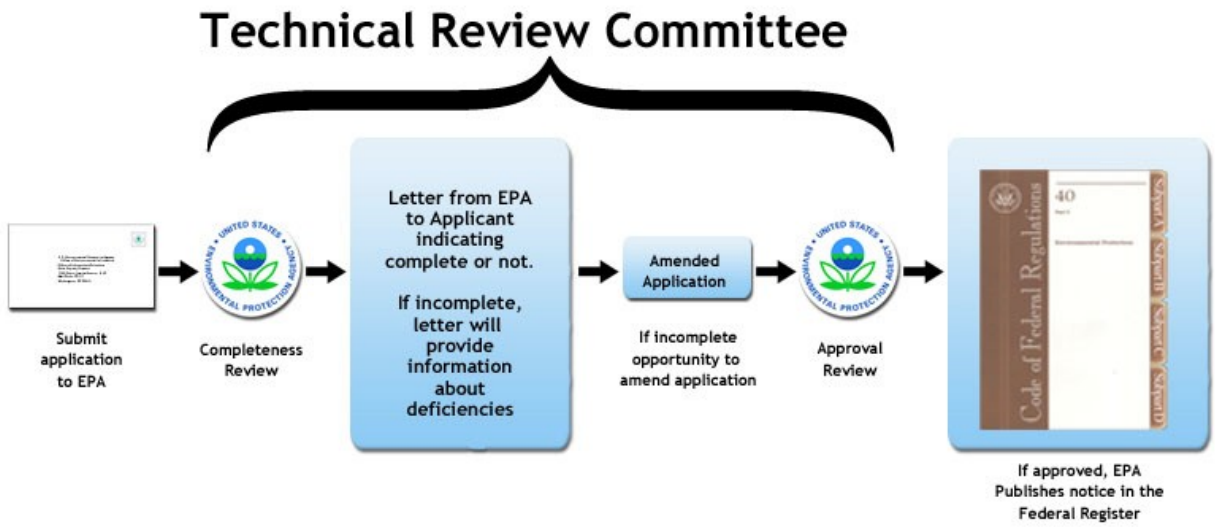
Phone: (202) 566-1175

And remember the application submission date requirements: Programs without an *existing e-reporting system must seek EPA approval *before* receiving e-reports. Programs with an existing e-reporting system were required to submit the application for EPA approval no later than January 13, 2010.

An "existing" electronic document receiving system receives e-documents in lieu of paper on or before October 13, 2005 or is substantially developed on or before that date as evidenced by establishment of system services or specifications by contract or other binding agreement.

LESSON 4: THE EPA REVIEW AND APPROVAL PROCESS UNDER PART 3

While Lesson 4 focused on the preparation and submission of an application using the CROMERR Part 3 process, this lesson describes what happens next, that is, the CROMERR application review and approval process.



Topics covered in this lesson include:

- The Technical Review Committee (TRC);
- EPA's Completeness Review;
- EPA's Approval Review;
- The Public Hearing Provision for Public Water System Programs; and
- Special Notes Regarding the Application Process.

TECHNICAL REVIEW COMMITTEE (TRC)

Applications formally submitted to the EPA are reviewed by an Agency-wide TRC, which includes representatives from the following offices:

- Office of Environmental Information (OEI);
- Office of General Council (OGC);
- Office of Enforcement and Compliance Assurance (OECA);
- Office of Air and Radiation (OAR);
- Office of Solid Waste and Emergency Response (OSWER);
- Office of Water (OW);
- Office of Chemical Safety and Pollution Prevention (OCSPP);
- Office of the Inspector General (OIG); and
- Each of the 10 EPA Regions.

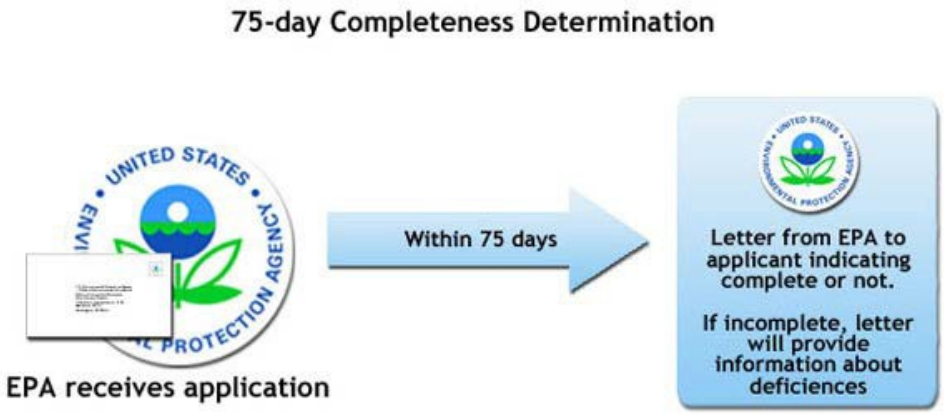
The TRC conducts both the completeness reviews and the approval reviews. The approval reviews conclude with a recommendation to the EPA Administrator, or their designee, to either approve or deny the application for program revision or modification.

Checking for Completeness

EPA first reviews an application for completeness, as described in § 3.1000(b)(3)(i)of CROMERR. Within 75 calendar days of receiving an application, EPA will send a letter to the applicant specifying whether or not the application is complete. For incomplete applications, the letter includes information on the application deficiencies.

States, tribes, and local governments may amend an application after EPA has determined the application package to be incomplete. For EPA to review an amended application, it must be resubmitted within "a reasonable period of time."

If application deficiencies are not remedied within a "reasonable period of time," EPA may act to approve or disapprove an incomplete application.

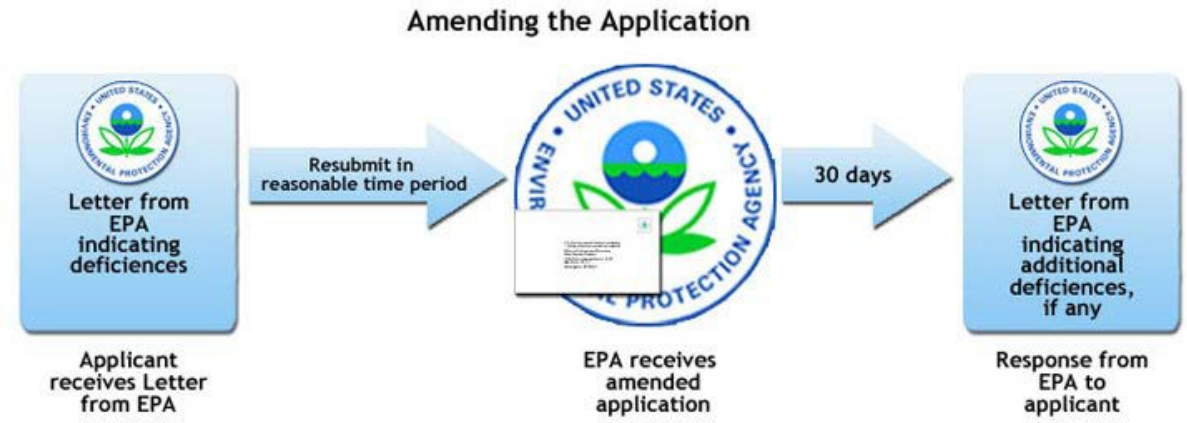


Resources:

- CROMERR § 3.1000(b)(3)(i)

Amending the Application

Applicants who receive a notice of deficiencies and then correct the issues in the application may resubmit the application. EPA then has 30 calendar days from time of receipt to respond with a new complete or incomplete determination.



Resources:

CROMERR § 3.1000(b)(3)(i)

Approval Review

Once EPA determines that an application is complete, the next step is to determine whether the application is approvable by reviewing it for compliance with CROMERR requirements spelled out in § 3.2000 of CROMERR.

For new systems, the Agency has 180 days from notification of completeness to conduct the approval review. If EPA does not act on a program revision or modification by the end of the 180-day approval review period, then that revision or modification is automatically approved.

For existing systems, the Agency has 360 days to evaluate the application for approval, and, again, failure to act before the review period ends results in automatic approval.

CROMERR does not require EPA to take the same action on all the program revisions or modifications in a consolidated application. EPA may approve some of the program revisions or modifications in the consolidated application, and disapprove others, as provided under § 3.1000(c)(2).

The approval generally becomes effective as of the date that EPA publishes a notice of the approval in the Federal Register.

If EPA does *not* take action within the allotted time period, the request for program revisions or modifications is automatically approved (unless the review period is extended at the request of the applicant).

RESOURCES:

- CROMERR § 3.1000(c);
- CROMERR § 3.1000(c)(4)(ii);
- CROMERR § 3.1000(d); and
- Sample EPA Response from the Federal Register.

PUBLIC HEARING PROVISION FOR PUBLIC WATER SYSTEM PROGRAMS

Applications for authorized public water system programs under Part 142 must provide the opportunity for a public hearing. Once EPA makes a preliminary determination to approve or deny the request for program revision or modification, EPA will publish a notice in the Federal Register. Requests for hearings must be submitted to EPA within 30 days after publication.

If a hearing is requested, EPA will announce the hearing in the Federal Register at least 15 days before the scheduled date. Based upon the results of the hearing, EPA will issue an order, either affirming or rescinding its preliminary determination, and will publish a Final Notice in the Federal Register.

If the order is to approve the program revision or modification, EPA's approval is effective upon publication of the Final Notice. However, if no hearing is requested, EPA's preliminary determination will be effective 30 days after the first notice was published.

RESOURCES:

- CROMERR § 3.1000(f) (PDF) (43 pp, 520 K)

Special Notes Regarding the Application Process

Remember that in consolidated applications, EPA is not required to take the same action on all revisions and modifications. For more information on this topic, reference § 3.1000(c)(2) of CROMERR.

Also note that authorized programs with approved program modifications or revisions to incorporate electronic reporting must apprise EPA of any changes (including laws, policies, and systems) that may affect program compliance with CROMERR requirements. For further information on this topic, reference § 3.1000(a)(4) of the CROMERR.

Resources:

- CROMERR § 3.1000(c)(2); and
- CROMERR § 3.1000(a)(4).

LESSON 5: CROMERR-COMPLIANT ELECTRONIC REPORTING

This lesson describes the legal, system, and procedural requirements for CROMERR-compliant reporting.

Topics covered in this lesson include:

- Valid electronic signature requirements;
- Requirements for systems that receive electronic reports:
  - Requirements for receiving any electronic report, and
  - Requirements for receiving electronic reports that include electronic signatures; and
- Additional enforcement-related requirements.

This lesson describes the various requirements as they are articulated in CROMERR.

INTRODUCTION: OVERVIEW OF CROMERR REQUIREMENTS FOR ELECTRONIC REPORTING

The purpose of the CROMERR requirements is to ensure that authorized programs that receive electronic documents in lieu of paper can rely on those documents for purposes of enforcement-related litigation.

Before examining the actual requirements, it is important to understand that their overarching purpose is to ensure that electronic reports can provide the same evidence of what was submitted—and of the submitter's and signer's intent—as their paper counterparts, particularly in support of civil or criminal litigation. This will be important, for example, where the government is prosecuting false or fraudulent reporting based on electronic submissions.

In CROMERR, these requirements are presented in three sections. Select each section below to learn more.

- Section 3.2000(a): Overall Requirements for Implementing Electronic Reporting provides an introduction to the requirements for using electronic reports in lieu of paper. It outlines that authorized programs must: (1) use an acceptable e-document receiving system that meets CROMERR standards; and (2) require that any e-document bear a valid e-signature if the signatory is required to sign the paper document, unless EPA has approved a process for handwritten signatures on separate paper submissions.
- Section 3.2000(b): Electronic Document Receiving System Requirements, the main focus of this lesson, provides the requirements for document receiving systems themselves. Again, it is important to remember that the purpose of the individual provisions of this section is to ensure that a system captures and maintains sufficient evidence to support the use of electronically received documents as evidence in civil or criminal litigation. The system must be able to demonstrate the authenticity of the reports it receives and any signatures these reports contain.

- Section 3.2000(c): Provisions of Enforceability contains the provisions to ensure that authorized programs can be enforced based on the receipt of electronic reports in lieu of paper.

Requirements for Authorized Program e-Reporting

§ 3.2000(a) states that authorized programs must use an acceptable electronic document receiving system, as specified by the criteria set forth in § 3.2000(b) and (c), which are described later in this lesson.

§ 3.2000(a) also requires that for any paper document that requires a signature, the corresponding e-document must bear a valid electronic signature. And it also outlines the conditions under which EPA will accept a paper follow on signature or certification as an alternative.

The next portion of this lesson will explain concepts while the remainder of the lesson will address CROMERR requirements for authorized program electronic reporting approaches.

Valid Electronic Signatures

Valid electronic signature refers to electronic signature on an electronic document that has been created with an electronic signature device. The identified signatory is uniquely entitled to use the signature device for signing that document provided that this device has not been compromised, and where the signatory is an individual who is authorized to sign the document by virtue of his or her legal status and his or her relationship to the entity on whose behalf the signature is executed.

CROMERR states that e-documents must have valid e-signatures if Title 40 requires handwritten signatures on the paper documents they replace unless:

- EPA approves the process by which the system accepts a hand-written signature on separate paper submission; and
- The signatory provides a handwritten signature.

Valid electronic signatures are explained in greater detail later in this lesson.

Standards for an Acceptable Electronic Document Receiving System

CROMERR requires that all acceptable electronic document receiving systems are able to generate legally-defensible data to prove document integrity according to the five standards below.

- **The e-document is not alterable without detection:** The system must be able to prove that its electronic documents cannot be altered without detection during transmission or at any time after receipt. This is a basic data integrity requirement that ensures what was sent is what was received.
- **Alterations to the e-document are documented by the system:** The system must provide a record of any alterations to the electronic document during transmission or after receipt.
- **The e-document can only be submitted intentionally:** The system must be designed so that the electronic document can only be submitted knowingly, and with intent, and not by accident.

- **Submitters and signatories can review the COR of the e-document:** Submitters and signatories must have: (1) the opportunity to review the Copy of Record (COR) in a human-readable format that clearly and accurately associates the electronic document information with descriptions; and (2) the opportunity to repudiate the electronic document based on this review.

  – **COR** refers to a true and correct copy of an electronic document received by an electronic document receiving system, which can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information. A COR includes:

    1. All electronic signatures contained in or logically associated with that document;
    2. The date and time of receipt; and
    3. Any other information used to record the meaning of the document or the circumstances of its receipt.

  – For example, if the COR is maintained as an XML file, then the COR should include the XSL style sheet used in conjunction with the file to present it back to the signer.

- **If an e-signature is required, then the e-document meets e-signature requirements:** If an e-document requires an e-signature, then it must meet the following requirements:

  – E-signatures must be valid at the time of signing.
  – E-documents cannot be altered without detection after signing.
  – Each signatory must have an opportunity to:

    - Review the e-document content, in human-readable format, before signing; and
    - Review the required certification statement, which includes criminal penalty implications of false certification, at the time of signing.

  – Signatories must sign either an electronic signature agreement or subscriber agreement for the e-signature device used to create his or her e-signature.
  – The system must automatically respond to the receipt of an e-document with an acknowledgement identifying the e-document received, the signatory, and the date and time of receipt. It must also be sent to at least one address that does not share the same access controls as the account used to make the electronic submission.
  – For each e-signature device, the identity of its unique user and the users' relationship to the entity for which he or she is signing has been determined by the state, tribe, or local government.

DEFINING "VALID ELECTRONIC SIGNATURES"

So what makes a valid electronic signature? A valid electronic signature on an electronic document is one that is created with an electronic signature device that is:

- Uniquely entitled to a signatory;
- Not compromised; and
- Used by a signatory who is authorized to sign the electronic document.

RESOURCES:

- The "Common Application Challenges" section of the CROMERR Application Challenges and Solutions (PDF) (19 pp, 292 K) guidance;
- Challenge Question Second Factor Approach (PDF) (3 pp, 161 K) guidance; and
- CROMERR Frequently Asked Questions (PDF) (8 pp, 187 K) guidance.

Valid electronic signature refers to an electronic signature on an electronic document that has been created with an electronic signature device. The identified signatory is uniquely entitled to use the signature device for signing that document provided that this device has not been compromised, and where the signatory is an individual who is authorized to sign the document by virtue of his or her legal status or his or her relationship to the entity on whose behalf the signature is executed.

Electronic signature device refers to a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

SYSTEM REQUIREMENTS FOR RECEIVING E-SIGNATURES

This lesson has already described the requirements for acceptable e-document receiving systems, per § 3.2000(b) of CROMERR. § 3.2000 also stipulates that systems receiving e-documents with e-signatures must also demonstrate certain functionality requirements. An approvable system must be able to provide proof of the following requirements.

THE SYSTEM MUST BE ABLE TO PROVE THAT THE E-SIGNATURE IS VALID AT THE TIME OF SIGNING.
When the document is signed, the e-signature must meet the requirements of a valid e-signature, as previously described in this lesson.

Note: This requirement must be met at the time the signature is executed.

THE SYSTEM MUST BE ABLE TO PROVE THE E-DOCUMENT CANNOT BE ALTERED WITHOUT DETECTION AFTER SIGNING.
E-documents with e-signatures cannot be altered at any time—during or after transmission—after signing without detection. A system must be able to prove that the document content is the same as the content at the time of signing. Currently, this generally involves some sort of encryption software.

Note: This requirement must be met at the time the signature is executed.

THE SYSTEM MUST BE ABLE TO PROVE SIGNATORIES HAVE HAD THE OPPORTUNITY TO REVIEW CONTENT. Before actually signing, signatories must have an opportunity to review the content for which their signature is being requested.

Note: This requirement must be met at the time the signature is executed.

THE SYSTEM MUST BE ABLE TO PROVE SIGNATORIES REVIEWED THE CERTIFICATION STATEMENT. Before actually signing, signatories must have an opportunity to review certification statements, including warnings that false certification carries criminal penalties, to establish that they understood the implications of their signature and meant to sign. This is important should someone ever be prosecuted for criminal fraud.

Note: This requirement must be met at the time the signature is executed.

THE SYSTEM MUST BE ABLE TO PROVE AN ACKNOWLEDGEMENT OF RECEIPT.
The system automatically sends an acknowledgment of receipt of the document to an "out-of-band" address. This is usually paper mail or an email address that does not share the same controls as those used to access the online submission account. This ensures that if, by chance, the signature device was compromised, the owner of the device will be notified outside of the system that someone made submissions in their name. This is a common practice used by online shopping sites—after making a purchase on a site, you are notified that the purchase was made with a confirmation in a separate email system.

Note: This requirement must be met at the time of signatory registration.

THE SYSTEM MUST BE ABLE TO PROVE SIGNATORIES HAVE SIGNED E-SIGNATURE AGREEMENTS.
Signatories have executed e-signature agreements related to using their signature devices. The e-signature agreement can be done electronically, but can also be done on paper.

The agreement must include the following:

- The signatory agrees to protect their signature device, such as a password or hardware token, from compromise;
- The signatory agrees to report any evidence of compromise; and
- The signatory understands that the signature they submit electronically with the device carries the same legal force and obligation as a hand written signature.

Usually, signatories execute this agreement when they register with the system to receive their electronic signature device.

Note: This requirement must be met at the time of signatory registration.

THE SYSTEM MUST BE ABLE TO PROVE IDENTITIES WITH LEGAL CERTAINTY.

This is a requirement that serves to establish the identity of an individual who is issued (or registers) an electronic signature device with enough evidence that it will hold up in a court of law. This is the one instance in all these requirements in which CROMERR is tiered in terms of priority and non-priority reports.

- For Non-Priority Reports, the requirement does not specify how identity proofing is to be carried out.
- For Priority Reports, the identity proofing must be done prior to signature execution, and must be done with one of two specified methods.

Priority reports and their associated identity proofing requirements will be discussed in more detail later in this lesson.

Note: This requirement must be met at the time of signatory registration.

PRIORITY VS. NON-PRIORITY REPORTS

Under § 3.2000(b)(5)(vii), CROMERR requires that more specific conditions be met where the electronically signed documents have been designated as Priority Reports.

Priority Reports are those that EPA has identified as likely to be material to potential enforcement litigation. Given this likelihood, it is important to provide not only for the provability of signature device ownership in principle, but for the practical need to make this proof with the resources typically available to enforcement staff and within the constraints of the judicial process in criminal and civil proceedings. A list of these reports can be found under Appendix 1 to Part 3 of CROMERR.

The CROMERR requirements for determining the identity of someone submitting an electronic report are different for Priority and Non-Priority reports. Select each of the buttons below for information on these requirements.

For **Priority** Reports, the system must determine identity before the e-signature is received by means of either:

- Wet-ink-on-paper e-signature agreements (i.e., subscriber agreements) either submitted to the state or maintained by a responsible company official. While some systems with CROMERR approval require that they be notarized, notarization is not a CROMERR requirement; **OR**
- Electronic identity-proofing by a disinterested party (such as a public key infrastructure [PKI] certificate authority or an agency official) using objectively verifiable information, including at least one government-issued identifier such as a driver's license number or passport; **OR**
- Identity-proofing using an approach no less stringent than electronic identity-proofing as specified above.

*Note: **Disinterested party** refers to an individual who is not connected with the person in whose name the electronic signature device is issued. A disinterested individual is not any of the following:*

- *The person's employer or employer's corporate parent, subsidiary, or affiliate;*
- *The person's contracting agent;*
- *A member of the person's household; or*
- *A relative with whom the person has a personal relationship.*

For **Non-Priority** Reports, the system must determine identity by collecting and maintaining information sufficient to prove the identity of individuals that sign and submit electronic documents.

Note that CROMERR does not specify **when** or **how** this goal is to be achieved.

Enforceability Provisions

In § 3.2000(c), CROMERR outlines the last of the requirements—the enforceability provisions for authorized programs implementing electronic reporting. Specifically, this section states:

- Failure to comply with the CROMERR e-reporting provisions subjects a person to penalties for non-compliance with the associated reporting requirement.
- E-signatures legally bind or obligate the signatory to the same extent as handwritten signatures.
- Proof that a particular e-signature device was used to sign an e-document will suffice to establish intent to sign the e-document and give it effect.
- Nothing in CROMERR limits the use of e-documents or information derived from e-documents in enforcement proceedings.

A program's compliance with these requirements is addressed in the AG Certification Statement, which was described in Lesson 3.

LESSON 6: USING THE CHECKLIST TO WORK THROUGH SYSTEM REQUIREMENTS

Lesson 5 described how CROMERR presents the system requirements for receiving electronic reports, with a focus on the system- and enforcement-related requirements.

Lesson 6 describes how these same requirements are presented in the CROMERR System Checklist (which was introduced in Lesson 4). You may want to refer to the checklist as you step through this lesson.

The CROMERR System Checklist describes the CROMERR system requirements as they affect the following five system processes:

1. Registration;
2. Signature Process;
3. Submission Process;
4. Signature Validation; and
5. COR.

This lesson covers these five processes in detail, and:

- Shows how the CROMERR requirements and checklist processes are interrelated; and
- Suggests how to use the CROMERR System Checklist Template in conjunction with the CROMERR System Checklist to describe how your system meets the CROMERR system requirements.

Note: The CROMERR System Checklist is not a required part of your CROMERR application; instead, it is a tool created to assist you as you work toward meeting the requirements.

Processes three and five are involved in electronic submissions, while processes one, two, and four are only involved where the submissions include an electronic signature.

REGISTRATION

Checklist items 1 through 4 are grouped under the Registration Process, where users establish their accounts in the system. This process typically requires users to provide information about them. The system administrator then reviews this information and provides the users with system privileges and signing credentials. Checklist items 1 through 4 represent CROMERR requirements that this registration process must satisfy.

1. **Identity-Proofing of Registrant**—For users who will sign electronic reports, CROMERR requires that the system determine the individual's identity, usually as a part of the registration process.

This identity-proofing is the one CROMERR requirement that is more stringent for users who will sign Priority Reports.

For users who will sign Priority Reports, CROMERR requires that the system establish their identity before accepting reports with their electronic signatures. There are two ways to do this. One is to establish identity through verification by, and attestation of, a disinterested party, based on identifiers—at least one of which is government-issued. The other way is to include the registrant's handwritten signature as part of the electronic signature agreement (ESA) process. Where the ESA is executed on paper with a handwritten signature, it is called a "subscriber agreement."

For users who sign only Non-Priority Reports, CROMERR does not specify when or how the identity proofing must be done, although either method specified for Priority Reports will satisfy the requirement in the non-priority case.

Reference: CROMERR § 3.2000(b)(5)(vii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

(vii) For each electronic signature device used to create an electronic signature on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; or

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; or

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

A **disinterested individual** is an individual who is not connected with the person in whose name the electronic signature device is issued. A disinterested individual is not any of the following: The person's employer or employer's corporate parent, subsidiary, or affiliate; the person's contracting agent; member of the person's household; or relative with whom the person has a personal relationship.

A **subscriber agreement** is an electronic signature agreement signed by an individual with a handwritten signature. This agreement must be stored until five years after the associated electronic signature device has been deactivated.

A **local registration authority** is an individual who is authorized by a state, tribe, or local government to issue an agreement collection certification, whose identity has been established by notarized affidavit, and who is authorized in writing by a regulated entity to issue agreement collection certifications on its behalf.

An **agreement collection certification** is a signed statement by which a local registration authority certifies that a subscriber agreement has been received from a registrant; the agreement has been stored in a manner that prevents unauthorized access to these agreements by anyone other than the local registration authority; and the local registration authority has no basis to believe that any of the collected agreements have been tampered with or prematurely destroyed.

2. **Determination of Registrant's Authority—**CROMERR requires the system to determine that users who will sign reports are actually authorized to do so on behalf of the specified regulated entities. This determination is usually based on some combination of the program's existing knowledge of the regulated entities, information submitted by the users or officials of the regulated entities, and some follow-up verification—such as phone calls or as a part of routine inspections.

Reference: § 3.2000(b)(5)(vii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

(vii) For each electronic signature device used to create an electronic signature on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; **OR**

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; **OR**

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

3. **Issuance (or Registration) of a Signing Credential in a Way that Protects it from Compromise—** CROMERR requires the system to provide users who will sign electronic reports with electronic signature devices (or credentials) to execute their electronic signatures. These devices could be passwords, PINs, PKI certificates associated with private-public key pairs, physical tokens such as a USB device, or devices incorporating biometrics (e.g., fingerprints). Whatever device is issued (or registered), there are two basic requirements that need to be met. The first is to ensure that a device intended for a specific, identified user is issued only to that individual. The second is to ensure that the process of issuing that device—and maintaining a record of it on the system—protects the device from compromise.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing"

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she

must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

4. **Electronic Signature Agreement**—CROMERR requires that users sign an Electronic Signature Agreement, and this is normally part of the registration process. This agreement must include language that obligates the registrant to protect the credential from compromise, and to immediately report any evidence of compromise to the system administrator. The agreement must also include a statement that the registrant understands that any electronic signature executed with the electronic signature device is as legally binding as a handwritten signature.

   Reference: § 3.2000(b)(5)(v)

   "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that… (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:…

   (v) Each signatory has signed either an electronic signature agreement or a subscriber agreement with respect to the electronic signature device used to create his or her electronic signature on the electronic document."

   An **electronic signature agreement** is an agreement signed by an individual with respect to an electronic signature device that the individual will use to create his or her electronic signatures requiring such individual to protect the electronic signature device from compromise; to promptly report to the agency... or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised; and to be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature.

   A **subscriber agreement** is an electronic signature agreement signed by an individual with a handwritten signature. This agreement must be stored until five years after the associated electronic signature device has been deactivated.

Signature Process

Checklist items 5 through 7 are grouped under the Signature Process and represent CROMERR requirements that this process must satisfy.

5. **Binding of Signatures to Document Content**—CROMERR requires that all electronic signatures be bound to the document content. This means that the system must provide a way to ensure that the document content is, in effect, "locked" so that it cannot be subject to undetectable changes once the signature is executed.

Reference: § 3.2000(b)(5)(ii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(ii) The electronic document cannot be altered without detection at any time after being signed."

6. **Opportunity to Review Document Content—**CROMERR also requires that the signature process provide the signers with the opportunity to review the content of the document they are signing.

Reference: § 3.2000(b)(5)(iii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(iii) Each signatory had the opportunity to review in a human-readable format the content of the electronic document that he or she was certifying to, attesting to or agreeing to by signing."

7. **Opportunity to Review Certification Statements and Warnings**—Along with the opportunity to review document content, CROMERR also requires that signers have the opportunity to review certification statements—including any applicable warnings of criminal penalties for false certifications—before asking them to execute their electronic signatures.

Reference: § 3.2000(b)(5)(iv)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(iv) Each signatory had the opportunity, at the time of signing, to review the content or meaning of the required certification statement, including any applicable provisions that false certification carries criminal penalties."

SUBMISSION PROCESS

Checklist items 8 through 12 are grouped under the Submission Process, and represent the CROMERR requirements that must be satisfied as the report or document is transferred to the system during a formal submission. Items 8 through 11 are required for all submittals, whether or not an electronic signature is included.

8. **Transmission Error Checking and Documentation**—CROMERR requires that the system be able to assure that it received the electronic report through an error-free transmission or that any errors in transmission are documented. This normally involves the use of cryptographic technologies (e.g., secure socket layer).

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

9. **Opportunity to Review COR**—CROMERR requires that the system provide the submitter and any signers with the opportunity to review the Copy of Record (COR) of the submittal after it is formally received. This is distinct from the requirement that signers have the opportunity to review document content and certification statements prior to signing and submitting, which are addressed in items 6 and 7. The requirement here has three elements. First, the system must

notify the submitter and any signers that the COR is available for their review. Second, the system must produce a version of the COR in a human-readable format. Third, and finally, the system must provide the signers and submitter with access to the COR in this human-readable format.

Reference: § 3.2000(b)(4)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(4) Any individual identified in the electronic document submission as a submitter or signatory had the opportunity to review the copy of record in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information and had the opportunity to repudiate the electronic document based on this review."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

10. **Procedures to Address Repudiation COR**—CROMERR requires that the submitter and any signers have the opportunity to repudiate the Copy of Record (COR) in part or in total, if they disagree with how the COR represents the submission. The system must also have a way to address any cases of repudiation and to document the history of the submission in those cases.

Reference: § 3.2000(b)(1)–(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

11. **Procedure to Flag Accidental Submissions**—CROMERR requires that the system be able to identify accidental or counterfeit submissions and have a way of addressing user repudiations of submissions as forged or accidental. For those cases, the system must also be able to document the submission's history.

    Reference: § 3.2000(b)(3)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

    (3) The electronic document was submitted knowingly and not by accident."

12. **Automatic Acknowledgement of Submission**—Where the submission includes an electronic signature, CROMERR requires that the system automatically send an acknowledgement to the individual identified as the signer at the time of submittal. The acknowledgement must identify the submittal, the signers, and the date and time the submittal was received.

    This automatic acknowledgement must be sent to an "out-of-band" address—that is, an address that does not share the same access controls like the username, PIN, or password—as the account used to make the electronic submission. This address is typically an email address, but it could be a U.S. Postal address or even a phone number.

    One purpose of this requirement is to help system users detect any compromise of their signature devices. If a submission includes a signature executed with a device by someone other than its registered owner, the owner will be alerted by the acknowledgement he or she receives at the out-of-band address. Given this purpose, the system must include procedures to follow-up when the acknowledgement cannot be delivered to determine whether the email or U.S. Postal address associated with the account is still valid.

    Reference: § 3.2000(b)(5)(vi)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to

generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(vi) The electronic document receiving system has automatically responded to the receipt of the electronic document with an acknowledgment that identifies the electronic document received, including the signatory and the date and time of receipt, and is sent to at least one address that does not share the same access controls as the account used to make the electronic submission."

SIGNATURE VALIDATION

Checklist items 13 through 17 are grouped under the Signature Validation Process, and represent CROMERR requirements that the system must satisfy as part of ensuring that electronic signatures it receives are valid.

13. Credential Validation—For each electronic signature received, CROMERR requires that the system verify that the identified signer is actually authorized to sign the submittal.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she

must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

14. **Signatory Authorization**—Under the Submission Process, CROMERR requires that the system be able to flag counterfeit submittals. Under the Signature Validation Process, CROMERR also requires that the system be able to flag counterfeit credential use, which would indicate that the credential has been compromised.

    Reference: § 3.2000(b)(5)(i)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

    (5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

    (i) Each electronic signature was a valid electronic signature at the time of signing."

    A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

    An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

15. **Procedures to Flag Counterfeit Credential Use**—CROMERR requires that the system include procedures to follow up on evidence and reports of credential compromise, including procedures to revoke a credential when compromise is indicated. Correspondingly, the system must be able to reject submissions that include e-signatures executed with revoked credentials.

    Reference: § 3.2000(b)(5)(i)

    "(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner,

including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

16. **Procedures to Revoke or Reject Compromised Credentials**—CROMERR requires that the system include procedures to follow up on evidence and reports of credential compromise, including procedures to revoke a credential when compromise is indicated. Correspondingly, the system must be able to reject submissions that include e-signatures executed with revoked credentials.

Reference: § 3.2000(b)(5)(i)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing."

A **valid electronic signature** is an electronic signature on an electronic document that has been created with an electronic signature device that the identified signatory is uniquely entitled to use for signing that document, where this device has not been compromised, and where the signatory is an individual... who is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed.

An **electronic signature device** is a code or other mechanism that is used to create electronic signatures. Where the device is used to create an individual's electronic signature, then the code or mechanism must be unique to that individual at the time the signature is created and he or she must be uniquely... entitled to use it. The device is compromised if the code or mechanism is available for use by any other person.

17. Confirmation of Signature Bindings to Document Content—Related to item 5—requiring signature binding—CROMERR requires that the system be able to determine whether the content of an electronically-signed submittal matches the content at the time the signature was executed.

Reference: § 3.2000(b)(5)(ii)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that…

(ii) The electronic document cannot be altered without detection at any time after being signed."

COPY OF RECORD (COR)

Checklist items 18 through 20 are grouped under the fifth and final process, the COR Process. These items represent CROMERR requirements that the system must satisfy in creating and maintaining CORs. The items address:

- What data CORs must capture;
- How access to CORs must be provided to program and enforcement staff; and
- How the CORs must be maintained.

18. Creation of COR—§ 3.2000(b)(1) through (2): For each legitimate submittal received, CROMERR requires the system to create a COR. The COR must be a "true and correct copy" of the submittal, in the sense that it must have exactly the same informational content as the submittal; otherwise, it must document any changes to this content after submittal.

The COR must include all associated signatures, the date and time of receipt, and any other information necessary to interpret the submittal.

Finally, the COR must be viewable in a human-readable format that makes the meaning of each information item clear; although it need not be maintained in this format or in the format in which the submittal was originally received.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

19. **Timely Availability of COR, as needed**—§ 3.2000(b)(1) through (2): CROMERR requires the system to provide program and enforcement staff with timely access to the CORs and the associated documentation.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures

contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

20. Maintenance of COR—CROMERR requires the system to maintain the CORs for as long as needed by program or enforcement staff. The CORs must be maintained together with any information needed to document their integrity, such as records or logs of associated signature validation processes. Finally, the CORs must be maintained in a way that protects them from alteration or deletion on a system that is electronically and physically secure.

Reference: § 3.2000(b)(1)—(2)

"(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that…

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented."

A **Copy of Record** is a true and correct copy of an electronic document received by an electronic document receiving system, which copy can be viewed in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or... labeling of the information. A copy of record includes: 1) All electronic signatures contained in or logically associated with that document; 2) The date and time of receipt; and 3) Any other information used to record the meaning of the document or the circumstances of its receipt.

THE CROMERR REQUIREMENTS AND THE CHECKLIST ITEMS

From the detailed discussion of the CROMERR System Checklist items, it should be evident that each checklist item corresponds to specific CROMERR requirements, and vice versa.

The tables on the next two pages make this correspondence explicit.

- The first table maps CROMERR requirements to the corresponding checklist items.
- The second table maps checklist items to the corresponding CROMERR requirements.

THE CROMERR REQUIREMENTS AND THE RELATED CHECKLIST ITEMS

System Requirements	Related Checklist Items
§ 3.2000(b)(1): The e-document is not alterable without detection.	Items 8, 10, 18
§ 3.2000(b)(2): Alterations to the e-document are documented by the system.	Items 8, 10, 18
§ 3.2000(b)(3): The e-document can only be submitted intentionally.	Item 11
§ 3.2000(b)(4): Submitters and signers can review the COR of the e-document.	Item 9
§ 3.2000(b)(5): If an e-signature is required, then the e-document meets e-signature requirements:	
(i) Signature valid at time of signing	Items 1, 2, 3, 13, 14 , 15, 16
(ii) Document cannot be altered without detection after signing	Items 5, 17
(iii) Opportunity to review content	Item 6
(iv) Opportunity to review certifications statement	Item 7
(v) Receipt Acknowledgement	Item 4
(vi) E-signature agreements	Item 12
(vii) Identity proofing with legal certainty	Items 1, 2

Mapping Processes and Checklist Items to Requirements

Checklist Items	System Requirement
Registration	
1. Identity-Proofing of Registrant	§ 3.2000(b)(5)(vii)
2. Determination of Registrants Signing Authority	§ 3.2000(b)(5)(vii) § 3.2000(b)(5)(i)
3. Issuance (or Registration) of a Signing Credential in a Way that Protects it from Compromise	§ 3.2000(b)(5)(i)
4. Electronic Signature Agreement	§ 3.2000(b)(5)(v)
Signature Process	
5. Binding of Signatures to Document Content	§ 3.2000(b)(5)(ii)
6. Opportunity to Review Document Content	§ 3.2000(b)(5)(iii)
7. Opportunity to Review Certification Statements and Warnings	§ 3.2000(b)(5)(iv)
Submission Process	
8. Transmission Error Checking and Documentation	§ 3.2000(b)(1)(2)
9. Opportunity to Review COR	§ 3.2000(b)(4)
10. Procedures to Address Submitter or Signatory	§ 3.2000(b)(1)(2)
11. Procedure to Flag Accidental Submissions	§ 3.2000(b)(3)
12. Automatic Acknowledgement of Submission	§ 3.2000(b)(5)(vi)
Signature Validation	
13. Credential Validation	§ 3.2000(b)(5)(i)
14. Signatory Authorization	§ 3.2000(b)(5)(i)
15. Procedures to Flag Counterfeit Credential Use	§ 3.2000(b)(5)(i)

Checklist Items	System Requirement
16. Procedures to Revoke or Reject Compromised Credentials	§ 3.2000(b)(5)(i)
17. Confirmation of Signature Binding to Document Content	§ 3.2000(b)(5)(ii)
COR	
18. Creation of COR	§ 3.2000(b)(1)(2)
19. Timely Availability of COR, as needed	§ 3.2000(b)(1)(2)
20. Maintenance of COR	§ 3.2000(b)(1)(2)

THE CROMERR SYSTEM CHECKLIST AND THE SYSTEM CHECKLIST TEMPLATE

The CROMERR System Checklist can help states that are preparing their CROMERR applications in two ways:

- First, it explains the CROMERR system requirements as specific system processes.
- Second, it provides an approach for documenting how a system meets CROMERR requirements, by describing how the system provides for each of the Roadmap items.

To support the second use of the checklist, EPA has also developed a corresponding CROMERR System Checklist Template—a document that provides a format for describing how the states system satisfies each of the checklist items. **While the CROMERR System Template is not required for application, EPA strongly recommends its use.**

For each checklist item, the template provides three blank spaces, for:

- Business Practices
- System Functions
- Supporting Documentation (a list of attachments)

Depending on the systems solution for the item, the description may fit into one, two, or all of these blanks.
The CROMERR Web site, at http://www.epa.gov/cromerr, provides several examples of how to use the CROMERR System Checklist Template to successfully document CROMERR-compliant systems for receiving electronic reports.

LESSON 7: FROM REQUIREMENTS TO SOLUTIONS

So far, this training has examined the CROMERR requirements in a couple of different ways. Lesson 5 presented the requirements as they are stated in the regulation. Lesson 6 examined the requirements by associating them with particular processes outlined in the CROMERR System Checklist.

Lesson 7 will provide another perspective on the requirements. It will provide examples of different approaches for meeting CROMERR requirements.

To help you choose solutions to comply with these requirements, Lesson 7 highlights:

- The relation between the CROMERR requirements and specific approaches to compliance; and
- Some key decisions in your compliance strategy that will affect your overall system design.

FROM REQUIREMENTS TO SPECIFIC SOLUTIONS

CROMERR REQUIREMENTS SET PERFORMANCE GOALS:

- They specify the **WHAT** your system must be able to do.
- But, they do not specify **HOW** your system does what it does—except, to a very limited extent, for the identity-proofing requirements in the case of Priority Reports.

CROMERR REQUIREMENTS DO NOT DICTATE SPECIFIC APPROACHES TO:

- System functions;
- Operating procedures;
- System architecture; and
- Technologies used.

While currently available technologies may limit the choice of solutions for some of CROMERR's requirements, the requirements are written to allow the range of choices to expand as new technologies and products emerge.

FROM REQUIREMENTS TO SPECIFIC SOLUTIONS

The task is to decide on particular solutions to meet the general performance goals.

Consider these two examples:

1. **CROMERR Requirement:** Provide an opportunity to review COR in a human-readable format.

- Requirement allows:
  - Delivery on paper, on magnetic or optical media, or electronically;
  - Delivery via online session, offline electronic transfer, or freight or postal carrier; and
  - Creation from data in a database or a copy of what was submitted.

- Solution could involve:
  - Printing to paper or disks;
  - Client-server transactions, file-transfer or email, or the U.S. Postal Service; and
  - XML or XSL formatting, PDF file capture, or other report generation functionality.

2. **CROMERR Requirement:** Issue (or register) a signing credential in a way that minimizes risk of compromise.

- Requirement allows:
  - Creation of credential by registrant, system, or third party; and
  - Credentials based on shared secrets (PINs or passwords), encrypted objects, biometrics, or physical tokens.

- Requirement could involve:
  - Cryptography, biometric readers, security of "secure socket layer" sessions, or the security provided by paper envelopes; and
  - Password- or PIN-generation functionality, enforcement of strength requirements for user-generated credentials, issuance and maintenance of user hardware, or interface with third party credential services.

From Requirements to Specific Solutions—Two Key Decisions

As you consider particular solutions to meet the general performance goals, two decisions are especially important because of their broader implications for your system.

These key decisions are:

1. Type of credential used; and
2. What the system defines as the COR.

Consider these key decisions before establishing system specifications and design. The following pages discuss these key decisions and describe their impacts on overall system design.

As you think about different approaches, remember the implications and trade-offs associated with each decision.

KEY DECISION 1: TYPE OF CREDENTIAL USED

Type of credential used determines:

- How Credentials are Issued—
  - Most credentials issued by or registered with the system require protection as they travel between registrant and system.
  - Credentials that are registered (rather than issued) may need the system to enforce strength requirements and—where issued by a third party—ensure authenticity.
  - Credentials that incorporate biometrics or include cryptographic keys will need specialized technologies to support them.
  - Credentials issued in connection with hardware tokens will require support for users' implementation.
- Approach to Binding Signatures to Document Content—
  - Credentials that include cryptographic keys may execute signatures that are automatically bound to the document being signed by incorporating a message digest or hash value uniquely related to the document content.
  - Other kinds of credentials lack this functionality, and so require an independent approach to signature binding.
- How Signatures are Validated—
  - Signatures executed with third party credentials require interaction with the issuing authority to determine that the credentials are authentic.
  - Credentials that provide cryptographic keys may require decryption functionality for validation of the signatures they execute.
- How Signatures are Included in the COR—
  - Credentials that are included "in the clear" in the signatures they execute (for example, as a PIN or password) need to be "shielded" in some way on the copies of record (COR), for example, by being encrypted or hashed.

Hash Value—Cryptographic hash functions are one-way mathematical algorithms that take an arbitrary length input and produce a fixed-length output string. The output is the hash value. A hash value is a unique and extremely compact numerical representation of a piece of data. It is computationally improbable to find two distinct inputs that hash to the same value (or "collide'').

For example, consider the following two types of credentials:

- Shared secrets in the form of PINs or passwords; and

- Certificates associated with private–public key pairs that are used to execute digital signatures.

Example Solutions ▸	**Solution A** **PINs or Passwords**	**Solution B** **Private–Public Key Pairs**
Issuing Credential	Requires Secure Socket Layer (SSL), Transport Layer Security (TLS) or another technology during setup to protect them as they travel between registrant and system.	The private key—which is used to execute the signatures—can be generated at the user's work station, so may not need to travel between registrant and system.
Binding Signature to Document Content	Execution of a PIN- or password-based signature does not bind it to the document signed, so the system must provide additional functionality to provide for signature binding.	The digital signature executed with the private key is bound to the document signed because the signature is just the hash value of the document content encrypted with the private key.
Signature Validation	Can rely wholly on internal system records of PINs or passwords registered or issued by the system.	Where the certificate associated with the key pair is issued by a third party—for example, where this is a PKI certificate—then validation requires interaction with the issuing authority to determine that the certificate is valid.
Including Signatures in Copies of Record	Signatures consisting of the PIN or password "in the clear" need "shielding" on the CORs—for example by being encrypted or hashed—so that PINs and passwords are not compromised by providing access to the CORs.	Access to a digital signature on a COR does not raise any issues of credential compromise because a digital signature does not include—and provides no way to derive—the private key needed to execute it.

Private–Public Key Pairs—Each user has a pair of cryptographic keys—a public key and a private key. The private key is kept secret, while the public key may be widely distributed.

Digital Signatures—A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped.

Public Key Infrastructure (PKI)—PKI enables users of a basically unsecure public network, such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

KEY DECISION 2: DEFINING THE COPY OF RECORD (COR)

What the system defines as the COR determines:

- How the COR is Shown to be "True and Correct"—
  - The closer the COR is to the file received, the easier a "true and correct" showing may be, since there will be few or no transformations of that file to account for.
  - For CORs that do not have an associated hash value, a "true and correct" showing will depend heavily on how their access is secured, controlled, and logged.
  - If CORs can incorporate changes to their content—for example, to accommodate submitter corrections—then a "true and correct" showing will depend heavily on a chain of custody that documents all such changes and their circumstances.
- How the Opportunity to Review is Provided—
  - The COR's format will determine what processing is needed for a "human-readable" version.
  - The medium in which the COR is maintained (e.g. electronic or paper) will affect how it can be provided for review.

For example, consider the following ways a system can define the COR:

- A PDF capture of the on-screen appearance of the file submitted, associated with the signature, the date and time of submission, and a hash value of the file submitted
- The submitted data as stored in a database, associated with the signature and the date and time of submission.
- A print-out of the submitted data, including the signature and the date and time of submission.

Example Solutions: ▸	**Solution A** **PDF Capture of the Submitted File**	**Solution B** **Data in a Database**	**Solution C** **A Paper Print-Out**
Opportunity to Review the COR	Requires making the PDF available online or sending it to the signer or submitter—as an email attachment or by other means—assuming the PDF captures a human-readable format.	Requires: (1) system functions to put the data into a human-readable format; and (2) making the formatted data available online or sending it to the signer or submitter by other means, such as an email attachment.	Requires procedures to: (1) receive requests; (2) produce paper copies; and (3) deliver the copies.
COR is Shown to be "True and Correct"	Requires a demonstration of the integrity of the PDF file, for example, by showing that it has been secured against tampering or that a hash value calculated from the file matches the hash calculated when it was received.	Requires a demonstration that: (1) the processing that placed the data in the database did not, in any way, affect its informational content; and (2) that the database has been secured against tampering and any undocumented changes.	Requires procedures to: (1) produce an accurate print-out of the submittal; (2) certify the print-out's accuracy; and (3) secure the print-out against any tampering or destruction.

FROM KEY DECISIONS TO CROMERR-COMPLIANT SOLUTIONS

To recap, two key decisions addressed in this lesson include:

- Decision 1—the type of credential you use; and
- Decision 2—how you define the COR.

These will determine the available solutions for many, if not most, of the CROMERR System Checklist items that express the CROMERR requirements for your systems.

In the next, and final, lesson, we will focus on four critical checklist items that have an especially close connection with these two key decisions.

LESSON 8: FROM KEY DECISIONS TO CROMERR-COMPLIANT SOLUTIONS

FOUR CRITICAL ROADMAP ITEMS

Lesson 8 focuses on four CROMERR System Checklist items that are closely related to the two key decisions discussed in Lesson 7, namely:

- Item 3: Issuance (or Registration) of a Signing Credential in a Way that Protects it from Compromise;
- Item 5: Binding of Signatures to Document Content;
- Item 13: Credential Validation; and
- Item 18: Creation of COR.

These four Roadmap items are especially important to assuring both that:

- CORs maintained by your system truly represent what was submitted; and
- Any associated electronic signatures can be proved to be authentic.

For each of these items, Lesson 8 provides both:

- General advice on how they can be addressed; and
- Specific examples of successful solutions drawn from already approved applications.

ITEM #3: ISSUANCE OF A SIGNING CREDENTIAL

As described in Lesson 7, Decision 1—the type of credential used—affects what is required to ensure that the credential is protected from compromise, as required by checklist Item 3. Item 3 is critical to proving the authenticity of the signatures it is used to create—if the credential is compromised, then there would be no way to control who may use it to create associated signatures.

Generally, the solution for Item 3 needs to include answers to the following questions:

HOW IS THE CREDENTIAL ISSUANCE PROCESS LINKED TO IDENTITY PROOFING (ITEM 1)?

If there is any uncertainty about who the credential was actually issued to (or registered for), then there is no way to tell who has it. Some approved systems send an email to the email address provided by the user on the Subscriber Agreement submitted to satisfy identify-proofing requirements.

In one approach to credential issuance, the link is provided by a verification key generated by the system and sent to the email address that the user provided on the Subscriber Agreement (which was submitted to satisfy identity-proofing requirements). The verification key is supplemented by requiring the user to enter the answer to a preset security question.

In another approach, the link is provided by a hyperlink generated by the system and sent to the email address that the user has provided on the Subscriber Agreement (which was submitted to satisfy

identity-proofing requirements). The hyperlink is supplemented by requiring the user to enter a password and provide the answers to two preset security questions.

WHAT KIND OF CREDENTIAL IS IT?

For example, is it a PIN or a password combined with the answer to a challenge question? Is it PKI certificate associated with a private–public key pair?

WHAT IS THE ACTUAL PROCESS FOR ISSUING OR REGISTERING THE CREDENTIAL?

What are the actual steps a user takes to receive or register his or her credential? Does the user log into the system or enter a password?

One process could involve having each user log on to the system with a verification key received via email, answer a security question, and create a password subject to password-strength requirements.

Another process could be to have the user log on to the system with the hyperlink received via email, provide his or her password, answer two security questions, and download the certificate package created by the PKI certificate authority.

HOW IS THE CREDENTIAL PROTECTED FROM COMPROMISE AS IT IS ISSUED OR REGISTERED?

That is, what kind of security is provided for the transaction (e.g., is SSL or TLS used)?

One approach could be to use a password creation session protected with SSL or TLS. An alternative approach could be to encrypt the private key and secure the download session with SSL.

HOW IS THE CREDENTIAL PROTECTED FROM COMPROMISE OR TAMPERING AS IT IS STORED IN YOUR SYSTEM?

That is, what kind of security is there, and does it include some kind of encryption of the credentials?

Some systems use passwords and security question answers that are one-way hashed, and stored in the system in that form. Other systems use a private key that is encrypted and stored only on the user's workstation. The private key may only be decrypted with a password available only to the user.

IS THERE A PROCESS TO ALLOW THE USER TO CHANGE HIS OR HER CREDENTIAL?

And if so, how does your system ensure that only the legitimate account holder is able to do this?

One process could require users who wish to change their password to enter the account's current password and answer a security question. Alternatively, in cases where the credential or password is lost or compromised, the user could be required to re-register and apply for a new credential.

ITEM #5: BINDING SIGNATURE TO DOCUMENT CONTENT

Both key decisions—type of credential and definition of COR—affect Item 5.

Recall that Decision 1—type of credential—affects signature binding in terms of the added functionality provided by PKI-based digital signatures. Decision 2—definition of COR—also affects this item. The COR will have to include both the locked document and the mechanism that provides the lock. Locking a document to be maintained as a discrete file will be very different than locking data elements in a database or on a paper printout.

Item 5 is critical to proving that the COR reflects what was signed and submitted. If the COR can be changed without detection after signature and submission, then there is no way to confirm the actual submission or to what the signer attested.

Generally, the solution for Item 5 needs to include answers to the following questions:

WHAT ARE THE STEPS IN THE SIGNATURE PROCESS?

For example, when does the signer provide the credential that executes the signature? What happens before and after? Which steps occur online or offline?

Signing could require an offline digital signature executed for the file containing the submission and an online entry of a password in conjunction with a review of the Certification Statement.

Alternatively, the process could include having a user log into the system by entering his or her password and answering a challenge question. The user would then be presented with the opportunity to review the document being signed and the certification statement. To sign, the user would then enter his or her password again and press a Submit button.

WHAT CONSTITUTES THE ACTUAL SIGNATURE?

For example, is it the PIN and answer to a challenge question provided by the signer? Or is it the digital signature created with the signer's private key?

Like the Signature Process, the signature could have two parts: a digital signature executed offline and a password entered by the user in conjunction with viewing the Certification Statement.

Or, the signature could simply be the password entered by the user.

AT WHAT POINT IN THE SUBMISSION PROCESS IS THE DOCUMENT ACTUALLY LOCKED, AND WHAT IS THE LOCKING MECHANISM?

For example, is the document locked by the execution of the signer's digital signature? Or is this a hashing function (or digital signature) executed by your system once the submission reaches your server?

For example, execution of the digital signature could lock the document. It would be created by calculating the hash value of the content being signed and then encrypting the hash with the user's private key.

Or, upon receiving the submission, the system could calculate a hash value for the submitted data file.

HOW ARE THE LOCKED DOCUMENT AND THE LOCK (E.G., THE HASH VALUE) INCORPORATED INTO THE COR?
For example, are these components of the COR?

The COR could include the document content (the locked document) together with its digital signature (the lock).

The COR could also include the submitted data file (the locked document) and the hash value (the lock) of that file.

HOW IS THE LOCK PROTECTED FROM TAMPERING?
For example, if the lock is a hash value, what would prevent someone with back-end access to your system from changing the COR, recalculating the associated hash, and substituting these for the originals?

The lock could be the user's digital signature, which is the hash of the document content encrypted with the user's private key. Someone who wishes to hide a change in the document content by replacing the lock with a new one would have to access the user's private key to execute a new digital signature with it. So, the security of the user's private key protects the lock from tampering.

Alternatively, the hash value could be protected from tampering by tightly controlled system access, redundant storage, and providing it back to the signer or submitter. Someone who wishes to replace this hash value with a recalculated version—to hide changes in the COR—would have to defeat system access controls and access all the copies of the original, including the one in the signer's or submitter's custody.

ITEM #13: CREDENTIAL VALIDATION

Decision 1—the type of credential used—affects what is required to validate it. Item 13 is critical to proving the authenticity of the signatures it is used to create. If the credential is not valid, then it may not belong to the signer identified in the submittal, or it may be compromised. In either case, there would be no way to prove that the identified signer is the individual who actually signed the submittal.

Generally, the solution for Item 13 needs to include answers to the following questions:

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL IS GENUINE—THAT IT WAS ACTUALLY ISSUED AS A PART OF THE REGISTRATION PROCESS?

In the case of PINs and passwords, this may simply be a matter of looking up the credential in a table maintained by the system. In the case of a third-party credential, such as a PKI certification issued by a certificate authority, this may require interaction with the third-party.

For example, a system could verify that the certificate presented by the user was issued by the organization and has not been placed on any certificate revocation list (CRL).

Or, a system could compare the hashed version of a password entered by the user with the hashed version the system stores with the user's account information to confirm that they match.

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL ACTUALLY BELONGS TO THE SIGNER IDENTIFIED IN THE SUBMITTAL?

For PINs and passwords, this may be a simple table look-up function, but for third-party credentials, this may require interaction with that party to verify identifying information embedded in the credential itself.

For example, a system could confirm that the identified signer is the individual identified by the certificate, which associates that person with a public key.

Or, similar to the way a system determines a credential is genuine, a system could compare and match the hashed version of a password entered with the hashed version of the password stored in the user's account.

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL WAS NOT COMPROMISED AT THE TIME OF SIGNATURE?

Addressing this issue normally requires the validation of a second-factor (known as second-factor authentication), which is some item uniquely within the control of the identified signer that can be used to prove that it was this individual—and no one else—who presented the credential to sign the submittal.

One approach to do this is to have the public key decrypt the digital signature, and thus confirm that it was executed with the associated private key. The private key would be protected by a password. To confirm that the password has remained within the exclusive control of the identified user, he or she would be required to answer a challenge question at log-in, which provides a second authenticating factor.

Or, a system could rely on a challenge question as a second authenticating factor in conjunction with a PIN- or password-based credential.

The most commonly used second-factor is the answer(s) to one or more pre-set challenge questions—although there are also more technologically sophisticated options available.

ITEM #18: CREATION OF COR

Both key decisions affect Item 18. Recall how Decision 2—definition of COR—affects the process of creating the COR and showing that it represents what was submitted. Decision 1—type of credential—

also affects Item 18. By helping to determine the Signature-Binding Process (Item 5), the choice of type of credential also affects how the COR can be shown to be a "true and correct" copy of the submittal.

Item 18 is closely connected with Item 5, and many successful applications address both items together under Item 5. In any case, both items are critical to proving that the COR reflects what was signed and submitted.

Generally, the solution for Item 18 needs to include answers to the following questions:

WHAT CONSTITUTES THE COR FOR YOUR SYSTEM?

If you have not addressed this question under earlier items (for example, under Item 5), Item 18 is the place to list, in detail, the components of the COR and how they are packaged together.

For example, the COR could include the submitted data, date and time of receipt, associated electronic signatures, and metadata to document the COR's integrity.

HOW DOES THE COR PROVIDE A "TRUE AND CORRECT" COPY OF THE SUBMITTAL—"TRUE AND CORRECT" REFERS TO HAVING THE SAME INFORMATIONAL CONTENT (BUT NOT NECESSARILY IN THE SAME FORMAT)?

The solution to this question may be closely related to the solution for Item 5, since, for example, the secured hash value that binds the signature to the document content may also help show that the COR containing this content is true and correct. A solution will also need to explain how the COR and any associated metadata (such as the hash value) are secured from tampering or destruction.

The contents of the COR could be digitally signed with a system certificate as soon as the submission is received, with both the digital signature and associated key secured by the system.

Or, the submission could be digitally signed at the user's workstation with a temporary private key that is not recoverable once the user session concludes. Decrypting the signature (with the associated public key stored with the COR) and comparing it with a recalculated hash of the signed document could assure the COR's integrity. Since the private key is not recoverable, no counterfeit signature could be generated to hide unauthorized changes to the COR.

HOW DOES THE COR INCLUDE ANY ASSOCIATED E-SIGNATURES, AND HOW DOES THEIR INCLUSION AVOID CREDENTIAL COMPROMISE?

CROMERR requires that the COR include any associated electronic signatures. When the signature includes the entry of a PIN or password, they are often included in an encrypted or hashed form to avoid compromising the PIN- or password-based credential.

For example, the COR could include e-signatures as hashed or encrypted passwords.

How does the COR preserve evidence of how it appeared to the signer when presented in a human-readable format?

If the COR is simply a PDF in a human-readable format, then this fact provides the answer. Otherwise, CORs for electronically signed submittals will need to include the formatting mechanism.

For example, if the COR is maintained as an XML file, then the COR should include the XSL style sheet used in conjunction with the file to present it back to the signer.

Additional Sample Solutions

The U.S. EPA CROMERR website includes a number of state-developed and approved CROMERR applications that are available for reference.

These sample applications include resources such as completed CROMERR System Checklists, completed Cover Sheets, and success stories of the related effort.

Another resource provided by EPA to help applicants is the CROMERR Application Challenges and Solutions document (first introduced in Lesson 3 of this training), which is available on the Tools for States, Tribes, and Local Governments page of the CROMERR site. This document describes common challenges identified in CROMERR applications but also provides examples of solutions used by CROMERR-approved systems.

All of these resources are provided by EPA to help applicants identify ways to meet CROMERR requirements.

Helpful Resources

Below is a list of the various tools and resources referenced in this training, which are also available through the CROMERR website.

Location	Description
Cover Sheet	This application cover sheet template provides a format for capturing specific and necessary information for the application.
CROMERR System Checklist Template	This 13-page template provides a format for capturing information regarding the system and how it meets specific CROMERR requirements.
Sample Successful Application Checklists	These are examples of EPA-approved application checklists that describe how the electronic document receiving system meets the applicable § 3.2000 CROMERR requirements and the application documents that provide an overview of the systems and the electronic submissions received by the

Location	Description
	systems.
CROMERR Application Challenges and Solutions	This document presents common challenges identified in CROMERR applications received by EPA. For each challenge, it presents the CROMERR issue or deficiency, examples of effective approaches to resolving them, and the EPA-approved systems that use these effective approaches. This document should be used by state and local environmental agency officials and system managers to help them in planning systems that are CROMERR-compliant, preparing CROMERR applications, and responding to notices from EPA of issues and deficiencies for submitted applications.
Challenge Question Second Factor Approach	This document describes the requirements and potential approaches to using a second factor. EPA has determined that to meet the CROMERR requirements for priority reports, a system using PIN or password must be accompanied by some other identifier that together with the PIN or password will be sufficient to prove that the e-signature has not been compromised. One approach is to use the PIN or password in conjunction with a challenge question to create an e-signature.
Fact Sheets	These files contain information about how CROMERR affects agencies, submission reports, and EPA offices in headquarters and regions.
CROMERR Definitions	This document contains a list of special terms used throughout the regulation.

U.S. EPA Disclaimer

Please note that each of the examples listed in this training provides an approach that could help satisfy the associated CROMERR requirement, depending on:

- How it is implemented; and
- How it is combined with approaches to meet the other CROMERR System Checklist items.

Adopting these example approaches does not guarantee that EPA will find the resulting system satisfies the CROMERR requirements.