



# Minnesota Pollution Control Agency

## STATEMENT OF WORK (SOW)-CR#2979 ADDENDUM

**Addendum No.:** One

**Date of Addendum:** March 15, 2010

**Due Date, Time:** March 23, 2010, 2:00 PM CDT

**Revised Date, Time:** N/A

**Project Title:** Consolidated Emissions Data Repository (CEDR)-Redesign

### SCOPE OF ADDENDUM

The purpose of this addendum is to REVISE the SOW and to answer questions received from potential Responders.

[Deletions are struck out and Additions are underlined.]

**The SOW is revised as follows:**

**1. Module 1-Web Application and Supporting Data Structures section is amended as follows:**

Module 1.6 – Delta and RAPIDS 3 data integration:

- 1) ~~The RAPIDS 3 database shall be converted to Oracle 10g database, if this work is not accomplished by the RAPIDS 3 team. This includes all database objects, including schemas, tables, views, functions, procedures, triggers and anything else required to enable the operation of the database both for the online system and for the RAPIDS 3 supporting applications.~~
- 2) 1) The System shall use DELTA as the master repository of AQ Permit Data, and RAPIDS 3 as the master repository of Emissions Inventory data. To the extent possible, data elements shall not be replicated across data systems. Tools needed to synchronize data between these systems shall be developed.
- 3) 2) The Air Quality Delta powerbuilder application shall be modified as necessary to accommodate changes to Delta database structure necessary to minimize data replication.

This addendum shall become part of the Statement of Work and **MUST** be signed and returned with Contractor's Proposal.

COMPANY NAME: \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

PRINTED NAME/TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

# Statement of Work Questions and Answers Pertaining to CR2979- Consolidated Emissions Data Repository (CEDR)-Redesign

**1. What is the skill set of the MPCA staff who can potentially be assigned to this task?**

MPCA staff will be proficient developers in web applications using .Net. They have participated in the construction and use of the MPCA online services framework which is the basis for the MPCA e-Government website, of which this project will be a part.

**2. Does the MPCA have PowerBuilder staff or should the responder plan to include PowerBuilder developers in their staffing plan?**

Having PowerBuilder staff is not a pass/fail criterion for responders. The MPCA may take this skillset into consideration when scoring the responses.

**3. What testing tools and methodologies do the MPCA currently use?**

The MPCA chooses testing tools and methodologies on a project-by-project basis, and has no pre-determined requirements established for this project.

**4. Will consultants need PowerBuilder skills?**

Refer to the response to question #2.

**5. With the MPCA completing development tasks on the Work plan, how can the vendor be responsible for 30 day bug free code?**

Part of the project is to develop the test plan (See page 12, Phase IV of the development plan) . This type of question will be addressed in the development of that test plan.

**6. Why is there no work allowed during the 10 day review and approval period after each of the 6 phases?**

The intent of the suggested work plan is to ensure that the contractor does not conduct unreimbursable work based on unapproved workplans. The suggested workplan does allow for some work to be done between certain phases when it is appropriate. The MPCA is open to suggestions in proposed work plans on how work may be expedited.

7. Does this mean there are only six payments throughout the project, at the end of each phase approval period?

No, reference Sample Work Order Contract section 3.2 under Consideration and Payment.

8. Can we have access to the information that the MPCA's planners generated in making up the proposal? We would like to know what THEIR expectations are for each of the six phases of the project, and how they arrived at their estimate of about a year. They have done a lot of work already to arrive at the conclusion that they can't do all the work themselves. Can we see that work during the project planning phase?

The background documents will be available to the selected vendor upon execution of the contract work order.

9. The Award criteria for the proposal is described as Total Low Cost Response Amount / Total Higher Cost Response Amount x Maximum Price. This infers that a total project price is required to be estimated before any of the project planning and design is complete.

Does the state plan to issue multiple awards with a multi-stage competition?

No

Does the state plan to allow for contract modifications based on discovery during planning and design phases?

Any changes/modification to the original executed Contract Work Order will be completed through the execution of a Contract Work Order Amendment. Refer to Section 8 of Sample Work Order Contract.

Is there a general guideline of percentage change expected/allowed?

No

10. The effort necessary to estimate the project requires more specific identification of the number of EI forms to be implemented. Is there a definition of the number and specific identification of EI Forms to be developed?

There are 6 different hard copy Criteria EI facility types; Registration B, C, D (2 types), Nonmetallic, and Large (type R). Please find the different types on the following website.

<http://www.pca.state.mn.us/air/emforms.html> Large facility (type R) forms are site specific and dependent on the number of emission units at the facility.

Availability of electronic reporting for Large facilities is the first priority.

Toxic forms are found on the following website; <http://www.pca.state.mn.us/air/toxics/toxics-dataguidance.html>. There are 3 different hard copy Toxic EI facility types; Registration C, D, and Large (type R).

Currently no forms exist for GHG although changes may be made per potential MPCA/EPA reporting requirements.

- 11. Is there any characterization/classification of the complexity for EI Forms to be developed? Are there existing work instructions/process descriptions for the EI Forms to be implemented? Is there any design information related to existing collection methods that can be provided to allow estimation of complexity of the EI Forms?**

Refer to the response to question #10.

- 12. Is business process definition complete for the implementation?**

Refer to the response to question #25.

- 13. Module 1.2, Items 6 & 7 What are the characteristics of the site specific data? How many possibilities are we talking about?**

Possibilities including the ones identified on page 3 Module 1.2 item 6) plus CEM, stack test, mass balance and other site specific data that is used for calculation of emissions and U.S. EPA Emission Inventory Schemas.

- 14. Will we be expected to use the MPCA change control system? If so, how much training/knowledge transfer is required?**

This issue will be addressed during the project planning phase.

- 15. Phase IV, item a) Can we use a structured set of documents as opposed to one development document? Is there a development system available that is equivalent to the production system?**

Yes. The details of the documents will be determined during the project.

- 16. Please confirm that vendors should propose a firm fixed price for the scope of work mentioned in this SOW and not time and materials. Yes or No?**

Reference Page 21 of SOW Section 5: Work Plan Cost Proposal

- 17. The SOW asks for a "separate email attachment" for the price proposal. Should the vendors submit 2 emails when submitting proposals (1) Technical Proposal and (2) Cost proposal? Yes or No?**

No, Provide one Work Plan Cost Proposal document as a separate **attachment** in e-mail response. Work Plan Cost Proposal must be titled as such and include company name.

- 18. Are vendors permitted to execute the tasks described in this SOW leveraging a vendor team that is based in both St. Paul, MN and Offshore?**

Refer to General Requirements Section page 25 of SOW Foreign Outsourcing of Work Prohibited.

- 19. My firm is a certified minority business enterprise. Will our firm receive 6% additional points when our proposal response is evaluated?**

If your firm meets the requirements specified in the Preference to Targeted Group and Economically Disadvantaged Business and Individuals in the General Requirements section of SOW and certification is verified your firm would received 6% of additional points based upon a 1,000 point scale.

20. According to the Per Diem/Travel section in the SOW, it appears that the State of MN will pay for travel and per diem in accordance with the Commissioners Plan. Please confirm that the State of MN will pay for vendor travel.

Reference Per Diem/Travel in the General Requirements section of SOW.

21. What is the State's budget for vendor provided services within the scope of this SOW?

The State has a projected budget for the services requested in this SOW.

22. Other than facility users, who else will be accessing the "Electronic Reporting System"?

Individuals who would be accessing the system would include MPCA staff, facilities, and representatives of facilities (consulting firms).

23. DELTA – What does it stand for? Both DELTA and AQ DELTA refers to the same system/database. Please confirm. If they are not the same, please describe the function and purpose of DELTA and AQ Delta and how they relate to each other.

Yes, Delta and AQ Delta are the same system, Delta is the parent data base which includes other media applications, AQ Delta is one of those applications

24. Currently, emissions information is manually entered into three separate emission databases". What are the names of these three databases? Per our understanding from the SOW documents, DELTA database, an MS-Access database, RAPIDS database and MS-Excel files are used to store the emission information in the current environment. Please clarify/confirm.

The 3 databases are: Delta (criteria pollutants except PM2.5), RAPIDS (air toxics and PM2.5) , and MS-Access (transition database to move registration permit data into RAPIDS), and MS-Excel (greenhouse gases).

25. Per "Air Emissions Inventory Redesign" PPT from the <http://www.pca.state.mn.us/air/cedr.html> website, the following documents/activities have already been completed by MPCA.

- Business object model –the 'what'
- Business process model(s) –the 'how'
- Identify internal and external user needs (Requirements)

**Can MPCA share the above documents/deliverable with the vendor community?**

Slide 12 in the presentation refers to the aforementioned documents as being sufficiently completed for the purpose of the MPCA selecting a category of solution (Slide 13) to move forward, e.g. contractor vs. in-house development. These documents are not available on the agency's website, but will be provided to the Contractor to conduct the document review mentioned on Page 8 of the SOW. Additional description of these documents is provided below:

Business object models– In June 2009, we conducted a joint application development session to do a high level map of the object. Participants included MPCA IT staff and staff from the criteria, air toxics and greenhouse gas inventory programs. Two business object model s were developed for:

- 1) Facilities- As defined on page 4 of the Project Definition (<http://www.pca.state.mn.us/publications/aq-ei1-02.pdf>)

2) Non-Facilities – Mobile and nonpoint sources as defined on page 4 of the Project Definition.  
Business process models – In fall 2009, MPCA staff developed 3 “As-Is” business process models: criteria inventory, air toxics inventory, and greenhouse gas inventory. “To Be” models were not developed as the MPCA expects these processes to change significantly with the availability of electronic reporting.  
Internal and external user needs- In summer and fall of 2009, MPCA staff conducted meetings with internal and external users to solicit information on their needs from an emission inventory system. The key needs identified in those sessions are described in the Module 1 of the System Component Requirements Requirements in the SOW (pages 2-4).

26. **As a follow-up to the above question, Did MPCA use an external vendor to gather requirements and document them? If yes, can you share the vendor information with us? Will that vendor be allowed to bid on this SOW? Please answer all three bullet-points.**

Refer to the response to question #25 for the first two parts of the question. Any contractor on the State of Minnesota’s Master Contract Program and approved in the listed Service Categories on page 1 of the SOW is eligible to propose.

27. **Per “Air Emissions Inventory Redesign” PPT from the <http://www.pca.state.mn.us/air/cedr.html> website, “Electronic Reporting System” must be completed by “Sept 2010” where as per SOW Page #16 “Project Milestones and Schedule” desired operational date of Module 1 is by December 31. Please confirm by which date the module 1 should be operational.**

As identified per SOW page 16 the desired operational date of Module 1 is by December 31, 2010.

28. **“this system must use the MPCA’s existing e-Government portal” – Does this refer to <http://www.pca.state.mn.us/> web site? If not please provide details about the MPCA e-Government Portal.**

The MPCA e-government portal is at <https://netweb.pca.state.mn.us/private>

29. **How do the Facilities and Consultants access the e-Government Portal?**

Refer to the response to question #28.

30. **Can you provide a copy of MPCA’s approved CROMERR Plan?**

Yes. See **Attachment A** at the end of this document.

31. **“development work .... using its own staff resources” – How many staff does MPCA have who have knowledge and experience in MPCA’s custom development framework?**

The MPCA has several qualified staff and will ensure that their time is available to support this project.

32. **“to decide how to allocate development work” – When would MPCA make this decision assuming that this contract is a fixed price by deliverables contract with the awarded vendor? How many MPCA staff would be used for Module 1 development?**

Refer to Phase III.b, page 10. The MPCA will make this decision as part of the design phase. The decision on resource will depend upon the system design.

**33. The high level functional scope of this SOW per our understanding is:**

- Covers ONLY Module 1 of the redesigned system
- Module 1 will address the development of an electronic reporting system by December 2010.
- As well as the development of tools needed to flow data from the DELTA to the electronic reporting system.
- And to transfer data from the electronic reporting system to the RAPIDS3 inventory database.

Please confirm our understanding and provide any additional details if required.

You are correct with your assumptions.

**34. The high level priority business requirements do not provide sufficient information for us to propose a "FIXED PRICE" solution. The requirements specified may lead to complex procedures, user interfaces, business rules and database integration.**

**So please provide more procedural details for each of the Module 1 requirement, so we can estimate properly.**

The amount of detail provided in the SOW is the amount of detail that we are prepared to deliver at this time. Respondents are free to make and document assumptions as part of their responses and these will be considered in the selection process.

**35. Has the State gathered detailed system requirements and prepared any documents for Module1? If yes, can you share the same with the vendor community?**

Refer to the response to question #25.

**36. "Potential exists for an amendment to this SOW to include Module 2 and 3 of this effort" – When would MPCA decide about amendment? What would be the factors in this decision?**

We expect to make this decision when the work associated with module 1 is nearing completion. Factors will include success of module 1, and resource availability.

**37. Please provide a copy of documentation(s) for "MPCA's Custom Application Development Framework". We need to understand the framework in order for us to estimate and propose a solution leveraging "MPCA's Custom Application Development Framework".**

We don't have any documentation to share at this time. Sufficient orientation will be provided as part of the contract execution.

**38. Questions regarding MPCA's Custom Application Development Framework:**

- **Is it .NET based framework?**  
Yes
- **What is the purpose of this framework?**  
To provide reusable components for online services.

- **What benefits does it provide to MPCA?**

See above

**Please provide an architectural overview of this framework.**

It is an n-tier online application development framework.

- 39. What is MPCA's estimation with respect to reusability of the existing MPCA development framework in CEDR project?**

This question to be addressed during the design phase.

- 40. How many onsite vendor resources can be accommodated by the State?**

We will be able to accommodate as many as the project requires.

- 41. Help – do we need to provide screen level help or field level help?**

Contractor will develop details in Project Plan.

- 42. Instructions – Does this refer to screen level instructions that would be provided on each screen to direct the users on the use of the system or does this refer to some thing else? Please provide clarification.**

Refer to the response to question #41.

- 43. FAQ – How many different types of FAQ to be provided? Will the FAQ be a static list of known questions or should it be dynamic?**

FAQ will be needed and will be updated as necessary.

- 44. Do you need a separate capability to maintain the FAQ list?**

Refer to the response to question #43.

- 45. "links to EI staff contact info" –**

- a. Are these links to external static web sites which would provide EI staff contact info?**

**We assume that there will be multiple links to the EI staff contact info based on the context. Please confirm and provide details if required.**

Contractor will develop details in the design of the new system.

- 46. "Specific entry portal for each type of permit" – Will these portals be public accessible or only accessible by authorized facilities and consultants?**

These portals will be accessible by authorized facilities and users only.

- 47. "Specific entry portal for each type of permit" –**

- a. Please provide the total number of types of permits should be provided with entry portals and provide list of those permit types.**

Refer to response to question #10.

**48. "EI Forms" – Please provide soft copies of EI Forms that the facilities currently use to manually report the emissions.**

Refer to the response to question #10.

**49. How many "distinct inventory forms" exist?  
Please provide a list.**

Refer to the response to question #10.

**50. Please confirm whether Vendor resource should provide services from Onsite at MPCA facility or offsite from Vendor facility.**

As per SOW page 7, "MPCA's Responsibilities," MPCA will provide work/meeting area.

**51. End Date – "Remaining deliverables provided by June 30, 2011" –  
a. What remaining deliverables does this refer to? Please provide details.  
Per our understanding the scope of this SOW (i.e Module 1 – Online Emission Reporting) will be completed by December 31, 2010. Please confirm.**

Refer to SOW page 5, "Module 2" and "Module 3" also refer to the response to question #27.

**52. What is the anticipated user acceptance testing duration for MPCA testing?  
Based on your knowledge of your user base and their locations etc., please let us know how many business days do we need to set aside to perform user acceptance testing.**

Contractor will develop details in test plan.

**53. Is "Load/Performance Testing" required for this project?**

Yes

**If yes, please confirm that the MPCA will provide the necessary testing tools for "Performance testing".**

If tools are required as part of the testing plan, the MPCA will be responsible for providing them.

**54. How many Subject Matter Experts (SME's) will be allocated to this project?**

Refer to page 16 of the SOW for response.

**55. How many hours per week of each SME is State planning to allocate for the project?**

Sufficient Subject Matter Expert resources for the project will be allocated to meet the schedule laid out in the SOW.

**56. For requirements gathering and definition, do we have to travel to multiple locations within Minnesota or will the requirement be provided to the Vendor in a MPCA central location?**

All meetings and work space locations will be held within or near the Minneapolis/St. Paul area.

**57. If travel required for requirement gathering, please provide the number of locations and the frequency of travel that we need budget for.**

Refer to the response to question #56.

**58. For User Acceptance Testing, do we have to travel to multiple locations within Minnesota or will the testing support be provided in a MPCA central location?**

Refer to the response to question #56.

**59. Will State provide travel expenses according to the State travel policies or should the vendor include travel expenses in the fixed price cost?**

Reference Per Diem/Travel section in the General Requirements of SOW and Section 5 Work Plan Cost Proposal under Response Requirements.

**60. Will MPCA provide normal office space, desktops, software, and hardware to the vendor resources performing services under this contract award? Please help the vendors understand what will be provided and what will not be provided?**

We will provide normal office equipment, including desks, chairs, computers and necessary software.

**61. Is State open for the following Offsite based delivery model?  
Onsite: Requirements Gathering, User Testing, Production Deployment and Training  
Offsite: Design, Development and Vendor Testing Please clarify.**

Yes.

**62. Will State provide the vendor resources VPN access to its systems for the purpose of remotely accessing State network for project purposes?**

Appropriate remote access can be provided.

**63. Please confirm that State will provide development, testing, acceptance and production environments for this project.**

Yes, we will provide sufficient environments.

**64. Who is responsible for deployment activities? Please clarify vendor responsibilities with respect to deployment/implementation activities? Please also provide the duration we need to set aside for deployment activities based on MPCA deployment process.**

The SOW states the responsibility is to be shared (see page 15). Respondents are encouraged to provide specific suggestions on roles and schedule in their responses

**65. Are there any warranty requirements for this SOW? If yes, please provide warranty requirements.**

See Phase IV.b last paragraph page 12.

**66. Is there a need to provide knowledge transfer of the new system to the State support personnel?**

**If yes, how many State resources should we transfer the knowledge to?**

Per page 15 of SOW, "contractor will develop and present training for MPCA staff, including system ..." The contractor shall train up to 10 MPCA staff.

**67. Is there a need to involve focus groups for the purpose of validating the requirements with them and to perform "Focus Group Testing"?**

**If yes, please provide the requirements for the same.**

Per page 7 and 8 of SOW, "contractor will review requirements."

**68. Can we propose to provide training on the train-the-trainer approach?**

**If yes, how many such training sessions should be included?**

Per page 15 of SOW, "contractor will develop and present training for MPCA staff, including system ..."

**69. Please confirm that the target date for completing Module 1 is December 31, 2010 as stated in the SOW. In the PPT document provided, the target date is specified as September 2010 (See slide 23) . Please clarify the schedule expectation.**

The target date for completing Module 1 is December 31, 2010, as stated in the SOW (page 16).

**70. After Module 1 implementation, Will MPCA continue to use DELTA for permit data management? Please clarify/confirm.**

Yes, after Module 1 implementation the MPCA will continue to use DELTA for permit data.

**71. Please confirm that after Module 1 implementation, MPCA will no longer enter EI data into DELTA?**

After Module 1 implementation the MPCA will no longer enter data or calculate emissions in DELTA.

**72. Please confirm that after Module 1 implementation, all EI data will be routed to RAPIDS 3 through the new system database (CEDR database)**

**Also please confirm that, to the extent required for item a above, we will need to develop data transfer modules to populate RAPIDS 3 database will EI data entered into CEDR database.**

RAPIDS 3 database is the CEDR database.

**73. In the TOBE model, What is the expected frequency of CEDR to RAPIDS3 data transfer?**

As often as needed.

**74. Please confirm that the new system database will be a centralized database to house the EI data including CAP, AT, Mercury and GHG before being transferred to RAPIDS3?**

Refer to the response to question #72.

**75. Please clarify the requirement Module 1.6 (1): Is it vendor's scope to migrate RAPIDS3 to Oracle 10g?**

- **When will MPCA make the determination as to whether this work is needed or not?**

- Please provide the RAPIDS 3 data model and list of all triggers, stored procedures and other schema elements in order for us to assess the scope of the data conversion effort.
- Please note that per information provided on Page 17 of the SOW, RAPIDS 3 is currently being developed and targeted for delivery by March 31, 2010. Hence do you anticipate the database conversion being in scope?
- Considering RAPIDS3 is targeted for delivery in March 2010, can you confirm whether the database platform is Oracle 10g or PostgreSQL?

**Reference Addendum No. 1 to Statement of Work (SOW) CR#2979.**

76. "Before testing is complete, the system must run for 30 days without defects"  
Typically during the testing phase, the development team would achieve one 'clean run' test cycle before releasing the system for acceptance testing. According to this requirement, should we perform one or more 'clean run' test cycles for a period of 30 days before releasing the system for acceptance testing?

This issue will be addressed during project execution in the development of the test plan

77. Before testing is complete, the system must run for 30 days without defects"
- Please clarify whether this pertains to system testing performed by the vendor before releasing system to user acceptance testing or does this requirement pertain to User Acceptance Testing?
  - Please note that this requirement is stated under the Development phase. Does this actually pertain to Testing phase?

That requirement applies to user acceptance testing. It is a requirement to guide the development of the Test Plan, which occurs during Phase IV, the development phase.

78. Considering the MPCA may allocate some of the development work to MPCA internal staff, how will MPCA determine accountability delineations between vendor and MPCA in the event of quality and/or productivity issues especially since the vendor may get paid under a fixed price deliverables based contract?

This will be addressed during project execution in the Development Plan.

79. Please provide list of specific browsers and their version numbers that need to be supported by this application?

IE 7 and 8, Firefox 3.x, Safari 4.x

80. Requirements Information provided in the SOW is at a very high level and hence it would be difficult to project a fixed cost estimate without understanding the details of the requirements and work responsibilities. Please note that, per statement provided in SOW page 7 (Phase II (a)) "The description of Module 1 in the System Component Requirements section above is the high priority requirements that have been elicited from internal (MPCA) and external stakeholders. This description is intended to represent a starting point".

Based on this, Can we provide a solution approach, where :

- a. We will provide a fixed cost estimate for the Phases I to III (Planning, Requirements and Design phases) and

No, Refer to Section 5 Work Plan Cost Proposal of Response Requirements.

- b. **We will have an opportunity to review and revise the development and testing estimates after the detailed system requirements have been defined and approved by MPCA?**

Refer to Section 8 of Sample Work Order Contract.

**81. "The data conversion program"**

- a. **Per our understanding the purpose of this data conversion is to migrate EI related data from the DELTA database to the new CEDR centralized database and Permit related data will continue to reside on DELTA database. Please confirm.**
- b. **If our understanding is incorrect, please clarify the scope of this data conversion.**

Your understanding is correct.

**82. The data conversion program"**

- a. **Please provide the data model of the existing database to be converted.**
- b. **How many tables should be migrated to the new database?**
- c. **What is the data volume for data to be migrated/converted?**
- d. **How many years of data should be converted?**

See SOW page 7, Phase II, a. "The work and deliverables for Requirements Verification and Validation."

- 83. "The data conversion program" - Please confirm that MPCA will be responsible for data cleansing activities since it would require business SME input to determine validity of data to be converted.**

Your assumption is correct.

- 84. Per page #2 of Project Definition document (provided in the link provided in the SOW), the business object model was developed using an external facilitation.**

- a. **Who developed the business object model?**
- b. **Can you provide a copy the business object model?**

Refer to the response to question #25.

- 85. shall consolidate on the form" – Does this requirement refer to a process of rendering and accepting different types of pollutants of a single permit type in a consolidated data entry form? Please clarify.**

See SOW page 3, Module 1.2 1)

- 86. "spreadsheet uploading" – What would be the format (CSV or Excel) of this spreadsheet file?**

Contractor will develop in the Requirements Verification and Validation plan.

- 87. "Print out paper EI forms" – Should the format of these printed forms look like the manual entry forms that are used in the current system?**

Format may or may not be the same as the existing forms depending on changes with Module 1.

- 88. "The Air Quality Delta PowerBuilder application shall be modified as necessary to accommodate changes to Delta database structure necessary to minimize data replication."**

- a. Please confirm that the scope of these changes will be limited to removing EI data entry related fields from DELTA to move them to new CEDR database.
- b. How many PowerBuilder components need to be changed?
- c. How many DELTA application screens will be impacted by these changes?
- d. Who will be responsible for regression testing the entire DELTA application after these changes?

Contractor will develop details to be determined.

89. Does existing MPCA portal provide screens to create and maintain user profiles?  
If yes, will it support creation and maintenance of Facility and other users of the "Electronic Reporting System"?

Yes and yes

90. Please provide the IIS Web Server version to be used for this project.

6.0

91. Please specify the .NET Framework version (3.5, 2.x, etc.) to be used for this project.

3.5

92. Please specify the Windows Server OS version (2003 or 2008) to be used for this project.

2003

93. Which Visual Studio IDE version (Visual Studio .NET 2005 or 2008) does MPCA use for .NET development?

2008

**94. Custom Reports:**

- a. Are there any requirements within "Electronic Reporting System" to generate customized reports?
- b. If yes, what is the name of the reporting tool that MPCA uses for reports development?
- c. Please provide list of reporting requirements needed in the new system.

Refer to page 7 of SOW, "Phase II: Requirements Verification and Validation." Reports will be needed and will be updated as necessary.

**95. Ad-hoc Reports:**

- a. Are there any requirements within "Electronic Reporting System" to generate ad-hoc reports?
- b. If yes, what is the name of the ad-hoc report generation tool that MPCA uses for ad-hoc reports development?

Refer to the response to question #94.

**96.**

- a. What is the anticipated total number of users of the "Electronic Reporting System"?

About 10 EI staff and about 2,200 facilities based on current inventory users. In addition, consultants hired by facilities will also be accessing the new system. This number could potentially increase if in the future additional facilities would be required to report greenhouse gas emissions.

- b. Please provide a list of user groups who will be accessing this new system.**

Refer to the response to question #96 a.

- c. What is the anticipated number of concurrent users (number of users accessing the application at the exact same fraction of time simultaneously) for the “Electronic Reporting System”?**

Refer to the response to question #96 a, although, potentially not all users would be accessing the application at the same time.

- d. How many EI reporting transactions are expected to be recorded per year through the reporting system?**

Refer to the response to question #96 a.

**97.**

- a. Please provide a soft copy of MPCA production environment technical architecture.**

This will be provided as an orientation during the project planning phase.

- b. Does MPCA use clustered servers to host Oracle and IIS?**

No.

- c. Does your current production environment support redundancies and fail over?**

No.

**98.**

- a. Did MPCA evaluate any COTS products for “Electronic Reporting System”.**  
**b. Did MPCA find any COTS product that meets this SOW requirements? Please provide details.**

There are no off the shelf software that meets the MPCA needs.

**99. Is MPCA looking for COTS or Custom based solution for this SOW?**

Refer to the response to question #98.

**100. How many onsite vendor resources does MPCA estimate for this project in each category viz Project Manager, Architect, Business/System Analyst, Programmer Analyst, etc.,?**

The resources provided in each of these categories by the MPCA are described in the SOW (page 16). The MPCA leaves it to the discretion of the Contractor to determine what onsite vendor resources are needed in each category to successfully complete Module 1 of the SOW.

**101. Please confirm that the contractor should assign a dedicated Project Manager for this project?**

Refer to the response to question #100.

**102. The contractor will review the documents on MPCA AQ DELTA data system, RAPIDS 3, .. and update where necessary"**

- a. Does MPCA have business process flow documentations for Criteria Pollutant and air toxics EI processes and GHG business processes?
- b. If yes, can you share those documentations with the vendor community?
- c. Please also include USEPA reporting requirements document.

Refer to the response to question #25 for parts a and b. USEPA reporting requirements are available on USEPA's website.

**103. Please confirm that the "External Stakeholders" will attend the requirements gathering sessions in a centralized MPCA location.**

The fifth bullet under Phase II (b) in the SOW (page 8) defines it as the responsibility of the MPCA Project Manager to "identify and communicate with external project stakeholders to gather input or schedule meetings as called for in the project plan." In previous input sessions at the MPCA's central office, external stakeholders have indicated interest in providing future input as needed.

**104. "Provide work area for Contractor's staff when on site" – Please provide the physical location of the MPCA office where contractor's staff will be working from.**

Work space will be provided in Saint Paul MN.

**105. The design must be organized based on the 6 sub-modules..." – Can we propose our own grouping of sub-modules based on our experience with similar web applications?**

Yes, see Page 5 last paragraph of the SOW.

**106. To facilitate requirements gathering sessions better and more productive, can we propose to deliver "Screen & Report Mock-ups" earlier than Phase III?**

Refer to the response to question #105.

**107. Deliverables 4 - "Hardware configuration modification recommendations and estimates"**

- a. Does MPCA already have a production environment with required capacity to host the new "Electronic Reporting System" and the associated databases?
- b. If yes, please provide documentations and/or diagrams for the production hosting environment with hardware/software specifications.

Yes. These will be provided during Phase I of project execution.

**108.**

- a. If MPCA staff resources participate in the development activities, who will assign work/task to them? MPCA or Contractor?

- b. Please confirm that if MPCA staff resources perform some of the development tasks, they will be available till the end of the project to complete the full development life cycle for the functionalities assigned to them.

The MPCA will assign MPCA resources. MPCA resource will be available for the full development life cycle.

**109. "a conversion test wherein the current active database will be test loaded into the new system"**

- a. Can we propose to load a sample set of data from the current active database instead of loading the entire current active database? This may be necessary to save time during multiple iterations of the System and Acceptance Testing.

Yes, you can propose that.

- b. Please clarify if MPCA prefers to have another approach towards this.

N/A

**110. "The contractor shall submit one electronic copy of the development document"**

- a. The expected content of this development document seems to be for the detailed design of the new system. Please confirm.

It is the detailed design including the actual code.

- b. Can we propose to develop the development document with the detailed design information such as E-R Diagram (LDM / PDM), Class Diagrams, Sequence Diagrams, etc., during Phase III instead of Phase IV?

Those elements would be appropriate in a phase III as the system design, and in phase IV as the as-built system.

**111.**

- a. Does MPCA have a development/SDLC process standard that is used for requirements gathering, design, development, testing and deployment of MPCA projects?  
b. If yes, please provide a copy of that to the vendor community.

We are not specifying a standard for this project.

**112. Is it MPCA intention to have multiple business releases for the "Electronic Reporting System"? If not, can you clarify what MPCA means by "Portions of this phase may be completed concurrently with phases IV and/or V"?**

We don't have specific intentions regarding release schedules. That statement is intended to provide the contractor with flexibility in the development of the Phase VI deliverables.

**113. Training:**

- a. Please confirm that the contractor provided training will only to the MPCA staff and not to the end users of the system.  
b. Please confirm that the scope of the training includes both functional and technical trainings.  
c. How much time (or number of training sessions) should we set aside for training?

Refer to the response to question #68.

**114. Final Technical Configuration Document:**

- a. Please describe the expected contents of this deliverable.
- b. Please provide a sample copy if available.

The Final Technical Configuration Document should describe the final data and application architecture, including data models and software configuration.

**115. System Maintenance Manuals:**

- a. Please specify a list of different types of manuals (such as User Manual, System Administration Manual, etc.) to be developed by the contractor.

The respondent should plan on developing two system manuals: One for non-technical MPCA staff system users, and one for technical staff responsible for system maintenance and administration.

**116. Can we include resumes only for the key contractor staff members with the proposal?**

Yes, you may include resumes for only the key contractor staff that would be providing services under this SOW.

**117. Would you consider a response if it proposes only alternative SDLC methodologies, a different basis for project costing and variations in the project timeline?**

Page 5, last paragraph, of the SOW, specifies that responses must include the specified six phase approach, but allows additional alternative proposals.

**118. Can you clarify the definition of "defect" and the process by which defects are identified and determined to require correction by the contractor? In particular, can you clarify how a "defect" would be differentiated from a "missed requirement" or "design defect" that has been reviewed and approved by MPCA in an earlier phase of the project? How would you ensure that a defect was not the responsibility of an in-house programmer contributing to the project? Will MPCA differentiate between critical defects that restart the 30 day testing period and non-critical defects that do not?**

We anticipate that these definitions and details will be determined in the development of the test plan.

**119. Do you intend to issue a fixed price contract by Phase? Would you consider a contract that allowed renegotiation of development, deployment and testing costs following requirements collection and/or following design? How would this affect the consideration of overall project cost as part of the evaluation criteria? Would you consider monthly invoicing for expenses incurred subject to a ceiling or fixed price?**

Refer to the response to question #80.

**120. If you intend to issue a fixed price contract by Phase, when would Phase 1 (project management) be considered complete? We assume that project management activities would occur throughout the contract and could be better suited to monthly invoicing (based on services performed). Are we correct in assuming that this bid is for costs through December 2010 which is the delivery date of Module 1?**

Refer to the response to question #7.

**121. Can you clarify the invoicing and payment schedule and required invoice documentation? For example, if**

**this contract is a fixed price per deliverable, the invoice would be one line item and not include a breakdown of labor and other expenses. However, the description under Section 3.2 of Consideration and Payment requires the breakdown.**

The Contractor shall submit invoices for completed work activities specified in the Work Order on a monthly basis to the MPCA with the required information listed in Consideration and Payment Section 3.2.

**122. Can you elaborate on the relationships of or provide high level information on the data flows between DELTA, RAPIDS 3, and CEDR?**

Per SOW page 2, "System Component Requirements"

**123. Under Phase V, item b, the SOW states that "the contractor will make improvements to the application until the MPCA is satisfied with the response time." What are the quantitative standards that MPCA will use to determine adequate response times so that the design and testing of the software can proactively address this requirement?**

This will be negotiated during the requirements phase.

**124. In Module 1.5, a human readable copy of EI submittals is required for CROMERR compliance. Are any other reports desired for either industry users or MPCA users?**

Refer to the response to question #94.

**125. Can more information be provided about the interface with the e-Government portal and framework, particularly for user authentication and authorization?**

Responders should assume that user authentication and authorization are sufficiently managed by the existing MPCA e-Government portal and framework, and that no additional development work is needed to meet those requirements for this project.

**126. How often will the system need to synchronize the inventory form with permit changes?**

The EI is a yearly cycle. Synchronization would need to be done on a batch process once a year and on an individual facility as needed basis.

**127. Which browsers (including version numbers) will need to be supported by the system?**

Refer to the response to question #79.

**128. In modules 1.2 and 1.3, the SOW mentions forms and storage for facility inventory and emissions information including units, throughput, control equipment, emission factors, emissions, and calculations. Will the system also be required to include forms and storage for release points and release point apportionment?**

Yes, the system would have to include release points and all other identified data elements from U.S. EPAs emission inventory schemas.

**129. The SOW alludes to administrative functions for adjusting data validation parameters in Module 1.4. Would additional administrative functions be desired that offer MPCA the ability to manage pollutants, emission factors, or code tables?**

Yes, contractor may develop details in Phase II, Verification and Validation.

**130. What is the format of the weekly status reports?**

The format of the weekly status reports is at the discretion of the Contractor to suggest in developing the communications plan portion of the Project Plan. (Page 6 of the SOW) The minimum expected frequency of communication on status is weekly. The MPCA is open to Contractor suggestions for the elements needed to have highly effective communication between the MPCA and Contractor during the project beyond this minimum frequency.

**131. What coding and development standards discussed in Phase IV.b (page 11) will be used to evaluate the source code?**

This issue should be dealt with during project execution, specifically in the development document.

**132. How does MPCA intend for incremental development and continual integration within the production environment to occur during Phase IV (i.e. prior to the start of Phase V Testing) as required in Phase IV.b (page 12)?**

The intent of the SOW is to leave the respondent sufficient flexibility to address this requirement in their response.

**133. Can you describe the custom application development framework required on page 17 paragraph 1?**

See reponse to questions 38 and 91.

**134. To meet the requirement for internal source code documentation on page 12 (3<sup>rd</sup> complete paragraph), would it be acceptable to include within each programming unit clear testing criteria and automated test code that would clarify the expected results of that piece of code?**

Yes.

**135. If a contractor objects to some of the General Requirements and/or provisions in the Sample Work Order Contract (pp 23 ff), can a bidder identify in its proposal specific objections and suggested revised terms that would be part of a negotiation process if the bidder is selected based on the evaluation process?**

Refer to Section 1 of SOW page 20; sub-section e) and f).

**Or, would that approach be deemed a non-responsive bid?**

Refer to Pass/Fail criteria page 19 of SOW.

Examples for the Sample Work Order terms are provided below (examples are not all inclusive, but provided for reference).

- A change to Section 1.2, "Expiration date," to read " \_\_\_\_: or until MCPA's acceptance of all deliverables, whichever occurs first."
- A rewrite of Section 5, "Correction of Deficient Work," to provide descriptive definitions of deficient work and provide specific mutual timeframes for correction of deficiencies.

# Attachment A: MPCA CROMERR System Checklist

<b>CROMERR System Checklist</b>	
<b>Item</b>	<p>GENERAL NOTES:</p> <ul style="list-style-type: none"> <li>• This MPCA CROMERR checklist is based upon the EPA approved NetDMR checklist. To facilitate EPA review of this checklist the MPCA used Microsoft Word "Track Changes" feature. An 'Edits Indicated Version' is also submitted as an attachment.</li> <li>• MPCA deviated as little as possible from the approved NetDMR CROMERR system checklist.</li> <li>• This MPCA CROMERR system checklist describes the system MPCA will use for all CROMERR compliant electronic reporting. To this end, we have made the following "mass" changes to the NetDMR checklist:               <ul style="list-style-type: none"> <li>○ "DMR" and "eDMR" changed to "CROMERR-compliant report" (references to report types)</li> <li>○ "NetDMR" changed to "MPCA-CROMERR" (as the name of our system)</li> </ul> </li> <li>• References to Java-specific implementation details have been deleted or replaced as appropriate to reflect that our system is built on the Microsoft .NET platform.</li> <li>• The NetDMR CROMERR Application Supporting Documentation has been incorporated into the appropriate sections of this MPCA CROMERR system checklist.</li> </ul>
<b>Registration (e-signature cases only)</b>	
<b>1. Identity-proofing of registrant</b>	
	<p><b>Business Practices:</b> MPCA-CROMERR will use a Subscriber Agreement. Per CROMERR 3.2000(b)(5)(vii)(C), the receipt of a signed Subscriber Agreement is sufficient proof of the user's identity. See Item 1 b-alt for more information on the Subscriber Agreement. The MPCA will review the information provided and perform additional identity proofing to the best of their ability.</p>
	<p><b>System Functions:</b> See Item 1 b-alt for more information on the information contained in the Subscriber Agreement and how the user would provide this information.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<b>1a. (priority reports only) Identity-proofing <i>before</i> accepting e-signatures</b>	
	<p><b>Business Practices:</b> See Item 1 for how identity proofing will be performed using a Subscriber Agreement. See Item 1 b-alt for more information on the information contained in the Subscriber Agreement, how the user will provide the information, and the verification business processes used by the MPCA to assure the requested access is appropriate for the user.</p>
	<p><b>System Functions:</b> MPCA-CROMERR will not allow a user's electronic signature device to sign electronic documents until a Subscriber Agreement has been received and verified by the MPCA. See Item 1 b-alt for more information on the information contained in the Subscriber Agreement and how the user would provide the information.</p>

	<b>Supporting Documentation (list attachments):</b>
<b>1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)</b>	
<b>1bi. (priority reports only) Verification by attestation of disinterested individuals</b>	
	<p><b>Business Practices:</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
	<p><b>System Functions:</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
	<p><b>Supporting Documentation (list attachments):</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
<b>1bii. (priority reports only) Information or objects of independent origin</b>	
	<p><b>Business Practices:</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
	<p><b>System Functions:</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
	<p><b>Supporting Documentation (list attachments):</b> N/A - use 1 b-alt Subscriber Agreement alternative</p>
<b>1b-alt. (priority reports only) Subscriber Agreement alternative</b>	
	<p><b>Business Practices:</b> Per CROMERR requirements, Subscriber Agreements will be stored for at least 5 years after the associated electronic signature device has been deactivated.</p> <p>See Item 1 and 1a for how the Subscriber Agreement meets the identity proofing requirements. See Item 2 for how the Subscriber Agreement is used by the MPCA to determine the requestor's signing authority.</p> <p>The Subscriber Agreement and any other related documents will be managed and maintained in the MPCA file system according to the MPCA retention schedule and file plan (a minimum of five years per CROMERR requirement).</p>
	<p><b>System Functions:</b> Per the definitions in CROMERR, a Subscriber Agreement is "an electronic signature agreement signed by an individual with a handwritten signature.". The user will complete portions of the Subscriber Agreement in an online MPCA-CROMERR form. The user will then print, sign, and mail the Subscriber Agreement to the MPCA. The user's electronic signature device will not be able to sign electronic documents until a Subscriber Agreement has been received by the MPCA and staff has verified the information (see Business Practices).</p>

The online MPCA-CROMERR Subscriber Agreement form requires the requestor to enter data specific to the MPCA-CROMERR form for which approval is being requested. At a minimum this data will include:

1. Full legal name.
2. Email address. The user will be required to enter their email address two separate times to assure it was entered correctly.
3. Phone number
4. The organization and facility for which the user is requesting signing privileges.
5. For each CROMERR-compliant report, whether the user has direct authority under the rules to sign the CROMERR-compliant reports for the organization and facility or the authority is being delegated to him/her.
6. If the authority is delegated, the name and title of the person delegating the authority.

The agreement includes language, in the first person, stating that the requestor:

1. Agrees to:
  - a. Protect their account password from compromise, not allow anyone else to use the account, and not share the password with any other person.
  - b. Promptly report to the MPCA any evidence of the loss, theft, or other compromise of the user account password and/or challenge questions.
  - c. Notify the MPCA if the user ceases to represent any of the requested facilities as the submitter for the organization's electronic CROMERR-compliant reports to MPCA-CROMERR as soon as this change in relationship occurs.
  - d. Review, in a timely manner, the acknowledgements (email and onscreen) and copies of submitted documents using their account.
  - e. Report any evidence of discrepancy between the document submitted, and what MPCA-CROMERR received.
2. Understands that he/she will be held as legally bound, obligated, and responsible by the electronic signature created as by a handwritten signature.

The user will then print, sign, and mail the Subscriber agreement to the MPCA. If the authority is being delegated to the requestor, the delegating authority must also sign the Subscriber Agreement.

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

**Supporting Documentation (list ):**

See attached Subscriber Agreement

**2. Determination of registrant's signing authority**

**Business Practices:**

The MPCA must receive a signed Subscriber Agreement from each user that is requesting the ability to sign CROMERR-compliant reports. Upon receipt of the Subscriber Agreement, the MPCA will verify the signatures through direct contact with the facility. MPCA will verify that the "Cognizant Official" is in the appropriate MPCA database for every facility the user includes in the Subscriber Agreement and that has been verified by the MPCA. The MPCA will retain a paper copy of the Subscriber Agreement on file according to item #1 b-alt. Upon verification, the MPCA will assign the appropriate level of access in MPCA-CROMERR.

The MPCA will validate that the requested CROMERR-compliant reports are valid for electronic reporting. Regulatory authorities will, to the best of their ability, validate the information provided to assure accuracy and that it is appropriate for the requestor to be granted signatory authority for the

	specified organization and facility. Once verification is complete, the MPCA will assign the user's account the appropriate MPCA-CROMERR signatory permission.
	<p><b>System Functions:</b> For information on the Subscriber Agreement, see Item 1 b-alt.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

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

	<p><b>Business Practices:</b> See Item 1 b-alt for the business processes used to process received Subscriber Agreements.</p>	
	<p><b>Business Practices:</b> I. MPCA-CROMERR provides the following mechanisms to securely issue signing credentials:</p> <ol style="list-style-type: none"> <li>1. The Subscriber Agreement contains language requiring the user to protect their signing credential, not share it with anyone else, and report any compromise to the MPCA (see Item 4 for more information on the contents of the signature agreement).</li> <li>2. The account creation process provides numerous levels of verification. The account creation process is as follows: <ol style="list-style-type: none"> <li>a. The Verification Key will be automatically generated by MPCA-CROMERR through the use of an algorithm that generates a random, globally unique key. The Verification Key will only be valid for only 7 days, after which the user will have to re-start the registration process.</li> <li>b. The registrant will be emailed a URL to verify their email address. The URL included in this email will link to a secure verification page (Secure Sockets Layer protocol v3). It will include the encrypted Verification Key as a query string parameter to allow MPCA-CROMERR to verify the validity of the key and immediately challenge the user with one of the security questions answered by the registrant during the registration process.</li> <li>c. After the registrant submits their information and MPCA-CROMERR emails the specified account, the user will be presented with a notification page indicating that he/she should receive the email within the next 24 hours, and that the registrant should contact the MPCA if he/she does not receive the email.</li> <li>d. The security question serves to link the original registrant with the user accessing the verification page and assure that the registrant has access to the specified email account. If an invalid account was specified, the original registrant would never receive the Verification Key and would not be able to verify the account. If the wrong person received the email, he/she would not know the answer to the secret question to verify the account.</li> <li>e. If the registrant enters the wrong answer to the security question 3 times, the verification process is locked, an email is sent to the registrant, and the user must contact the MPCA to continue (or create a new account).</li> <li>f. The registrant must set a password during the verification process. The password must be between 8 and 100 characters and contain upper- and lower-case letters and numbers. Once the password is changed the Verification Key is no longer valid.</li> <li>g. Only verified accounts have access to MPCA-CROMERR beyond the verification page. Verified accounts have limited access to MPCA-CROMERR until the MPCA grants the account signatory rights to a CROMERR-compliant report for an organization and facility.</li> <li>h. The registrant's password and responses to the security questions are stored in the database in a hashed format using a secure hash algorithm (SHA-256). One-way hashes are designed to prevent the retrieval of the pre-hashed data (or something else that hashes to the given hash) given just the</li> </ol> </li> </ol>	

hash. This significantly reduces the possibility of learning the password or security question responses by gaining access to the database.

- i. A random XXXXXX-character password salt is created for each password using the NET RNGCryptoServiceProvider class. The salt is appended to the password and the resulting string is hashed (SHA-256) and the hash is stored in the MPCA-CROMERR database. For more information on salts see <http://msdn.microsoft.com/msdnmag/issues/03/08/SecurityBriefs/>. The use of a salt primarily strengthens the protection of passwords as follows :
  1. The addition of the user specific salt to each user's password assures the salt+password combination for each user is unique. A one-way hashing algorithm is designed to assure that the hashed forms of any two distinct values do not hash to the same value (defined as a collision). While such collisions do occur, the likelihood of such collisions is remote. The use of a salt makes it extremely unlikely that two users who have the same password will have the same hashed password.
  2. Makes it extremely difficult to use a pre-generated list of hashed common passwords to determine a user's password. A malicious user would need to know the user's salt value to create a pre-generated list of hashed passwords for each user.
3. The request for signatory rights provides numerous levels of verification. The MPCA-CROMERR process for requesting and receiving signatory rights is as follows:
  - a. Only verified accounts can request or be granted signatory access to a CROMERR-compliant report for an organization and facility.
  - b. If a malicious user intercepts the verification email, knows the answer to the secret question, and is able to access MPCA-CROMERR prior to the intended registrant he/she would still need to complete, print, sign, and mail the Subscriber Agreement to the MPCA before he/she would be able to submit a fraudulent CROMERR-compliant report. This would require the malicious user to know the user's applicable CROMERR-compliant reports as well as for each report the corresponding organization and facility name, and then submit forged Subscriber Agreement.
  - c. If a malicious user performed the steps in (b), the intended recipient would be able to detect the compromise. Since users are required to set a new password when using a Verification Key, the intended registrant would receive an email notification of a password change that he/she did not make. Also, when the intended registrant attempts to use the provided Verification Key he/she would be notified that the key had already been used.
  - d. The verification business process used by the MPCA is described in Item 1 b-alt.

## II. MPCA-CROMERR provides additional credential protection throughout the lifetime of the account:

1. MPCA-CROMERR requires all users to provide the answer to five security questions at the time a user registers to use the system. The list of available questions will be provided by MPCA-CROMERR. The questions will be chosen such that the expected answers should be common knowledge to the user, but should not otherwise be readily available (e.g., found on Google). For example, questions could include: "The make and model of the first car I owned" or "The name of my first pet". A list of at least ten questions will be provided to the user. The questions and answers are stored within the MPCA-CROMERR database. The questions will be stored in plaintext. The answers will be hashed using the SHA-256 algorithm. Wherever the user is required to provide the answer to a security question, MPCA-CROMERR will randomlyXXXXXX choose one of the security questions on file for the user. The answer provided by the user will be hashed and compared to that stored in the database.
2. Users can change their password, security questions, and security question answers at any time through MPCA-CROMERR. Users must reenter the account's password and answer the security question prior to changing any account information.
3. MPCA-CROMERR requires users to change their password every 90 days to something that has not been one of the account's past 10 passwords.
4. An Account is locked after three unsuccessful login attempts, three unsuccessful attempts to sign a CROMERR-compliant report, or three unsuccessful attempts to change account information within a 24 hour period Once locked:
  - i) The account can not be used to log in to MPCA-CROMERR.
  - ii) An email is sent to the user to notify them that the account was locked. If the account was locked due to unsuccessful login attempts, as opposed to the MPCA locking the account due to suspected compromise, the user can have the account unlocked by either providing the answer to a security question or contacting the MPCA. If the account was locked for any reason other than exceeding the number of unsuccessful login attempts, the user must contact the MPCA to have the account unlocked.

	<p>iii) An email is sent to the MPCA describing the potential problem.</p> <p>5. When a locked account is unlocked, the process outlined in 1.2 will be performed to change the password. A new Verification Key will be generated and emailed to the user. The user will not be able to log into MPCA-CROMERR until he/she visits the verification page and resets the account password.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>
<p><b>4. Electronic signature agreement</b></p>	
	<p><b>Business Practices:</b> See Item 1b-alt</p>
	<p><b>System Functions:</b> MPCA-CROMERR will use a Subscriber Agreement, which is defined as "an electronic signature agreement signed by an individual with a handwritten signature". The content of the Subscriber Agreement is described in Item 1 b-alt.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

<p align="center"><b>Signature Process (e-signature cases only)</b></p>	
<p><b>5. Binding of signatures to document content</b></p>	
	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b></p> <p><b>Signature Process</b> The signature process is a multi-step process. MPCA-CROMERR will create a unique Copy of Record (COR) for each CROMERR-compliant report that is submitted. MPCA-CROMERR also allows users to upload supporting documentation (i.e., attached files) that should be associated with the CROMERR-compliant report. The process used to create the COR and handling of attachments are detailed below.</p> <p><u>Data Document</u></p> <ul style="list-style-type: none"> <li>• The data document is created for each submitted CROMERR-compliant report. The data document is an XML document where the XML tags provide semantic meaning to the data. The document includes, at a minimum:             <ol style="list-style-type: none"> <li>1. All the user-provided data for the CROMERR-compliant report.</li> <li>2. Legal Certification Statement to be displayed to user during signing process (see Item 7).</li> </ol> </li> </ul> <p><u>Signing the Document</u></p> <ul style="list-style-type: none"> <li>• Users must indicate which of the CROMERR-compliant reports displayed on the Verification page he/she intends to sign (e.g., through a checkbox next to each CROMERR-compliant report).</li> <li>• MPCA-CROMERR will randomly choose one of the secret questions on file for the user's account. The user must enter the account's password and provide the answer to the question in order to sign the CROMERR-compliant report.</li> <li>• If the user enters the wrong password or answer to the secret question 3 times the account will be locked</li> </ul>

and can not be used until it is unlocked. See Item 3 for more information on how the account can be unlocked.

#### Hash Algorithm

- MPCA-CROMERR uses SHA-256 to generate all hash values. This is the current approved FIPS standard.

#### Confirmation Number

- A unique confirmation number is generated based on the user account information, IP of user, and current system date. The confirmation number is unique to the submission. If multiple CROMERR-compliant reports are submitted by the user at the same time, each CROMERR-compliant report within the submission will have the same confirmation number.

#### Submission Receipt

- A submission receipt is created for each CROMERR-compliant report that is submitted. The submission receipt is an XML document where the XML tags provide semantic meaning to the data. The receipt includes
  1. Confirmation Number
  2. The hash of the data document
  3. Hashes of each attached file
  4. Metadata about each attached file (e.g., name, type, etc)
  5. Date/Time of the submission
  6. Identifying information from the signing account, including:
    - a. The user's full name
    - b. Account Number
    - c. Email Address
    - d. Hashed Password (at time of signing)
  7. IP of submitting computer.

#### Copy of Record (COR)

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

#### COR Signature

- Each MPCA-CROMERR installation will have an RSA 1024 bit asymmetric key that will only be used for an MPCA digital signature (e.g., not used to establish SSL connections).
- MPCA-CROMERR will use its private key to digitally sign the CORs. The signature will be executed against a message digest created from the COR using the SHA-256 hashing algorithm.

#### Confirmation Page/Email Acknowledgement

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

#### **COR Alteration Protection**

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

### Use Case A. Signatory Falsification

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

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

*Mitigation:* This use case is mitigated as follows :

- It is computationally infeasible for the user to forge the digital signature without the private key
- The MPCA-CROMERR private key will be protected from unauthorized access by storing it in a secure location on the MPCA-CROMERR server. Physical access to the server will be restricted as specified in Item 20.
- A MPCA-CROMERR administrator is required to specify which key pair on the server MPCA-CROMERR will use for digital signatures. MPCA-CROMERR will log any changes made to the key/pair used by MPCA-CROMERR for signing CORs.

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

### Use Case B MPCA Staff Falsification

*Description:* An MPCA staff member alters the COR in MPCA-CROMERR without the signatory's knowledge. A possible scenario includes an attempt to alter a Signatory's submission from being compliant to non-compliant.

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

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

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

### Use Case C. Third Party Modification

	<p><i>Description:</i> A third party alters the COR in MPCA-CROMERR without the knowledge of the MPCA or signatory. A possible scenario includes a group attempting to alter a submission from being compliant to noncompliant in an attempt to cause enforcement actions against a facility or organization.</p> <p><i>Mitigation:</i> Without the cooperation of the signatory or an internal staff member, all mitigation strategies applied to Case A and Case B would apply to this use case. In addition, the malicious user would need to gain access to the network on which MPCA-CROMERR is installed.</p>
	<b>Supporting Documentation (list attachments):</b>

## 6. Opportunity to review document content

	<b>Business Practices:</b>
	<p><b>System Functions:</b>  During the signing and submission process (See Item 5), the user will be presented with a verification page. The verification page includes:</p> <ol style="list-style-type: none"> <li>1. A read-only view of the CROMERR-compliant reports the user selected. The data will be displayed in a manner that provides the user the opportunity to review the data, but does not require the user to review it. For example, the CROMERR-compliant report may be displayed in a summary format with the ability for the user to expand the CROMERR-compliant report to display all the information.</li> <li>2. Links to download and view any documents that were attached to the CROMERR-compliant report.</li> <li>3. Checkboxes to confirm selection of the CROMERR-compliant reports to be signed and submitted.</li> <li>4. Certification statements (see Item 7).</li> <li>5. A text box for supplying the account password.</li> <li>6. A randomly selected security question on file with the user's account and a text box to supply an answer.</li> </ol>
	<b>Supporting Documentation (list attachments):</b>

## 7. Opportunity to review certification statements and warnings

	<b>Business Practices:</b>
	<p><b>System Functions:</b>  During the signing and submission process (See Item 5), the user will be presented with a verification page. The verification page includes :</p> <ol style="list-style-type: none"> <li>1. Information in Item 6.</li> <li>2. A certification statement (in the first person) stating the user: <ol style="list-style-type: none"> <li>a. Is the owner of the account he/she is using.</li> <li>b. Has protected the account and password and is in compliance with the Subscriber Agreement.</li> <li>c. Has the authority to submit the data on behalf of the facility and organization.</li> <li>d. Agrees that providing the account password to sign the document constitutes an electronic signature equivalent to his/her written signature.</li> <li>e. Understands this attestation of fact pertains to the implementation, oversight, and enforcement of a federal environmental program and must be true to the best of the user's knowledge.</li> <li>f. Current password is not compromised now or at any time prior to the submission.</li> </ol> </li> <li>3. A certification statement appropriate to the MPCA.</li> </ol> <p>Example language: provided by Michael Ledesma (EPA/OECA) that would appear to meet most of 2a,2b,2e,and 2f:</p>

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

**Supporting Documentation (list attachments):**

### Submission Process

#### 8. Transmission error checking and documentation

**Business Practices:**

**System Functions:**

See Item 5 for the submission process and more detail on how the submission process protects against alterations once it has been received by MPCA-CROMERR.

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

1. No alteration of the document content is expected during transmission or after it is received. MPCA-CROMERR will create and display an MD5 hash of the submitted document so the user can verify that what was received is what was sent.
2. The entire session takes place over the Secure Sockets Layer (SSL) protocol v3. This protects against man-in-the-middle attacks.
3. The information in the data XML document used for the verification page (see Item 5) comes from data already stored in the MPCA-CROMERR database. No updates to this data are performed at any time during or after the submission process. With the protection in place from man-in-the-middle attacks, this provides a high level of assurance that the user is seeing the data as it is stored in the database.
4. The data XML document and all attached files are included, without alteration, in the COR. This assures that the COR contains the same data, in the same format, as what the user was given the opportunity to review (see Item 6).
5. The COR signature (see Item 5) is provided to the user in an email acknowledgement along with instructions to access the COR. The email allows the user to detect modifications to the submission. See Item 5 for more information.
6. It is computationally infeasible for the user to create a valid COR signature without the MPCA-CROMERR private key. This protects against users modifying the COR and attempting to claim the data were altered in MPCA-CROMERR (see Use Case A in Item 5).
7. The validity of the signed COR can be determined using the MPCA-CROMERR public key. This assures that the MPCA-CROMERR private key was used to sign the COR.
8. The data hash and COR signature can be recomputed, if needed, to compare against the original values.
9. The submitter has the opportunity to review the data during data entry, the submission process, and the COR review process.

**Supporting Documentation (list attachments):**

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

##### 9a. Notification that copy of record is available

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b>  Submitters are informed and made aware of the availability of CORs in multiple ways:</p> <ol style="list-style-type: none"> <li>1. The submitter is automatically sent an email notification after each submission. The email contains information on how to access the COR.</li> <li>2. Submitters have the ability to view CORs at any time using MPCA-CROMERR. This will be documented in the MPCA-CROMERR help system and manual.</li> <li>3. After each login, the user is presented with a list of the past 10 login sessions including the date/time and whether any CROMERR-compliant reports were submitted during the session. If submissions were made, a link to view the CORs of the submissions will be included.</li> </ol> <p>For information on how a user would view the COR see Item 9c.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

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

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b>  See Item 5 for information on what is contained within the COR. The COR is a zip file which contains all the appropriate information for the submission. The documents within the COR are of two types:</p> <p><u>XML Documents</u>  The XML tags used in these documents relate the user-supplied data to the context in which the data were provided. Item 5 for more information on the contents of the XML documents.</p> <p><u>Attached Files</u>  Users can attach supporting documents to the submission. These documents are stored in their native format. For example, a Microsoft Word document will be stored in the COR file as a Microsoft Word document. The user is required to have the appropriate application to view the attached file. For example, users must have Microsoft Word or a program that can understand the Word format in order to view the Word document.</p> <p>See Item 9c for how users can view the COR.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

**9c. Providing the copy of record**

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b>  MPCA-CROMERR creates the COR, a zip file, during the submission process . See Item 5 for more information on the process for creating the COR and the contents of the COR. Signatories are notified of the COR in an email acknowledgement and on the confirmation page during the submission process. The email includes instructions for viewing the COR. The confirmation page contains both a link to download the COR as well as a link to view the COR online. All users with appropriate access for a particular CROMERR-compliant report can view the CORs for that CROMERR-compliant report. They can view submitted CORs by logging into</p>

	<p>MPCA-CROMERR and searching for CORs for the specified CROMERR-compliant report.</p> <p>The COR can be presented in a human-readable format in two ways:</p> <ol style="list-style-type: none"> <li>1. <u>Download</u> MPCA-CROMERR allows users to download the COR. After unzipping the COR, the user can apply the XSL stylesheet to the Data XML document to present it in a friendlier html format and view all the supporting documents that were attached to the CROMERR-compliant report submission.</li> <li>2. <u>Online Viewing</u> MPCA-CROMERR would provide a mechanism to allow user to view the contents of the COR online. NetDMR would automatically unzip the submission zip file to retrieve the files. The user can view the Data XML document, with the XSL stylesheet applied, and download any supporting documents that were attached to the CROMERR-compliant report submission. The user is required to have the appropriate application installed to view the attached file. For example, users must have Microsoft Word or a program that can understand the Word format in order to view the Word document.</li> </ol> <p><b>Supporting Documentation (list attachments):</b></p>
--	---

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

	<p><b>Business Practices:</b> The anticipated reasons a user would want to repudiate a COR include :</p> <ol style="list-style-type: none"> <li>1. The data submitted is incorrect, and a correction needs to be provided.</li> <li>2. The user did not submit the COR.</li> </ol> <p>MPCA-CROMERR allows users to replace a CROMERR-compliant report previously submitted through MPCA-CROMERR. Users can also replace attachments that were previously submitted. Therefore, users should not repudiate a MPCA-CROMERR submission due to incorrect data. Instead, he/she should submit a corrected CROMERR-compliant report, which would generate a new COR. In this manner, the entire history of the CROMERR-compliant report, including all corrections, will be documented.</p> <p>If the user did not submit the COR, the user's signature device has been compromised. The user is required to immediately lock his account to prevent additional compromises and contact the MPCA. After calling the MPCA, the extent of the compromise will be assessed to determine whether any additional submissions need to be repudiated. The signatory and the MPCA will also investigate how the account may have become compromised in order to prevent future occurrences. The MPCA will flag each - fraudulently submitted COR as repudiated.</p>
	<p><b>System Functions:</b> The help system will document the repudiation process.</p> <p>The system allows the MPCA to flag CORs as repudiated.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

**11. Procedures to flag accidental submissions**

	<p><b>Business Practices:</b> If a user determines that he/she accidentally submitted a CROMERR-compliant report, the submission can be corrected with a follow-up submission.</p>
	<p><b>System Functions:</b> MPCA-CROMERR provides multiple mechanisms to prevent accidental submissions :</p> <ol style="list-style-type: none"> <li>1. MPCA-CROMERR performs a QA analysis on each CROMERR-compliant report to validate that all required data points are provided. Only CROMERR-compliant reports that pass the QA analysis can be submitted.</li> <li>2. The MPCA-CROMERR submission process uses a multi-step approach to reduce the likelihood of</li> </ol>

	<p>accidental submissions.</p> <ol style="list-style-type: none"> <li>a. Users must select the CROMERR-compliant report(s) they intend to submit.</li> <li>b. Users are given the opportunity to review the selected data in a read-only manner.</li> <li>c. Users must confirm their intent to submit by providing their password and security question answer on the verification page.</li> </ol> <p>3. While it is unlikely that a user will proceed through the submission steps accidentally, in such a case, there are additional mechanisms in place to assist the user in identifying and correcting an accidental CROMERR-compliant report submission:</p> <ol style="list-style-type: none"> <li>a. Submitters are sent an email after every submission.</li> <li>b. A list of previous logins is displayed every time a user logs in. The login list indicates whether or not a submission was made during that session.</li> <li>c. Users can review the CORs of all previous submissions using MPCA-CROMERR.</li> </ol> <p>MPCA-CROMERR maintains all CORs for the retention period specified in Item 20.</p> <p><b>Supporting Documentation (list attachments):</b></p>
--	--

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

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b> MPCA-CROMERR sends an acknowledgement email to the email address on file for the submitter after every submission. An email log is kept to track that the acknowledgement was sent.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

**Signature Validation (e-signature cases only)**

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

**13a. Determination that credential is authentic**

	<p><b>Business Practices:</b></p>
	<p><b>System Functions:</b> MPCA-CROMERR will compare the hashed form of the user-supplied password (appended with the user salt) and the hashed form of the answer to the secret question provided during the signing process to the hashed form of the user's password and the hashed form of the user's response to the secret question stored in the database. See Item 3 for more information on the user password salt.</p>
	<p><b>Supporting Documentation (list attachments):</b></p>

### 13b. Determination of credential ownership

**Business Practices:****System Functions:**

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

**Supporting Documentation (list attachments):**

### 13c. Determination that credential is not compromised

**Business Practices:**

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

**System Functions:**

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

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

**Supporting Documentation (list attachments):**

### 14. Signatory authorization

**Business Practices:**

See Item #2 for the process MPCA-CROMERR Administrators use to grant signatory authority to MPCA-CROMERR users.

**System Functions:**

The MPCA-CROMERR authorization system includes a "submit" role that grants permission for a user to sign a CROMERR-compliant report. This role is associated with a user and each CROMERR-compliant report for which he/she has signatory authority. MPCA-CROMERR uses the authorization system to determine whether a given user is authorized to submit a given CROMERR-compliant report.

**Supporting Documentation (list attachments):**

### 15. Procedures to flag spurious credential use

	<p><b>Business Practices:</b> Administrators will periodically review the results of the fraud analysis and the login logs to determine if an account has been compromised. If it is determined that a compromise has occurred, the affected account will be locked, preventing the user from signing CROMERR-compliant reports, and the user will be contacted to address the situation.</p> <p><b>System Functions:</b> MPCA-CROMERR includes functions that allow MPCA-CROMERR Administrators to detect the possibility that a user's device has been compromised:</p> <ol style="list-style-type: none"> <li>1. Each time a user logs in to MPCA-CROMERR, the IP and date/time of the login is stored. Inconsistencies in the logins, such as different IP addresses may indicate a compromised password.</li> <li>2. MPCA-CROMERR will only allow a user to maintain a single concurrent MPCA-CROMERR session. If the user is already logged in, the previous login will be invalidated. If overlapping login attempts are frequently made, it may indicate a compromised password.</li> <li>3. MPCA-CROMERR will include fraud analysis functionality, in which the logs are periodically analyzed for irregularities. Irregularities will be flagged for MPCA-CROMERR Administrators to investigate and take further action, if appropriate. The irregularities MPCA-CROMERR will flag are: <ol style="list-style-type: none"> <li>a. Inconsistencies in the logins, such as use of multiple IP addresses.</li> <li>b. Frequent overlapping login attempts from different IP addresses.</li> <li>c. Irregular submission patterns. An example of an irregular pattern would be a user who has submitted a single CROMERR-compliant report every month for the past 6 months, but then submits 50 in one month.</li> </ol> </li> </ol> <p>MPCA-CROMERR includes functions that allow MPCA-CROMERR users to detect the possibility that their account has been compromised.</p> <ol style="list-style-type: none"> <li>1. After each CROMERR-compliant report is submitted the submitter is sent an email acknowledging the submission.</li> <li>2. After logging in to MPCA-CROMERR, a list of the user's previous logins is displayed, including the date/time of the login and whether or not a submission was made during that session.</li> </ol> <p>If it is determined that a compromise has occurred, the user is required to lock their account and notify the MPCA.</p> <p><b>Supporting Documentation (list attachments):</b></p>
--	---

**16. Procedures to revoke/reject compromised credentials**

	<p><b>Business Practices:</b> An investigation will begin within one business day of when an account is suspected of being compromised. The investigation will determine whether a compromise has occurred. If it is determined that the account has been compromised, the account will be immediately locked.</p> <p><b>System Functions:</b> Users are able to lock their account and MPCA-CROMERR administrators are able to lock any user's account. A user or administrator will lock the user account if evidence suggests the account has been compromised. A locked account can not be used to sign a CROMERR-compliant report or log in to MPCA-CROMERR.</p> <p><b>Supporting Documentation (list attachments):</b></p>
--	--

**17. Confirmation of signature binding to document content**

	<p><b>Business Practices:</b></p>
--	-----------------------------------

	<p><b>System Functions:</b> MPCA-CROMERR submitters will not use digital signatures to sign electronic documents. Instead, submitters will use a password. The submission process is provided in Item 5. As described in the process, identifying account information from the submitter's account will be inserted into the COR of the submission to bind the submitter's signature to the document content.</p> <p>The signature binding will be confirmed and the document integrity verified by recalculating the signature of the COR and comparing it to the signature generated at the time of submission. If any part of the COR was altered, including the signature binding information, the new signature would differ from the original.</p> <p><b>Supporting Documentation (list attachments):</b></p>
<b>Copy of Record</b>	
<b>18. Creation of copy of record (See 18a through 18e)</b>	
<b>18a. True and correct copy of document received</b>	
	<p><b>Business Practices:</b></p> <p><b>System Functions:</b> See Item 5 for the contents of the COR and the process used to assure it is a true and correct copy of the data.</p> <p><b>Supporting Documentation (list attachments):</b></p>
<b>18b. Inclusion of electronic signatures</b>	
	<p><b>Business Practices:</b></p> <p><b>System Functions:</b> See Item 5 for the contents of the COR and information on how the electronic signature is included in the document.</p> <p><b>Supporting Documentation (list attachments):</b></p>
<b>18c. Inclusion of date and time of receipt</b>	
	<p><b>Business Practices:</b></p> <p><b>System Functions:</b> MPCA-CROMERR includes the date and time of the submission in the COR. See Item 5 for more information on the contents of the COR.</p>

	<b>Supporting Documentation (list attachments):</b>
<b>18d. Inclusion of other information necessary to record meaning of document</b>	
	<b>Business Practices:</b>
	<p><b>System Functions:</b>  The COR is a zip file which contains all the appropriate information for the submission. See Item 5 for more information on what the COR contains. The documents within the COR are of two types:</p> <p><u>XML Documents</u>  The XML tags used in these documents relate the user-supplied data to the context in which the data were provided. Item 5 for more information on the contents of the XML documents.</p> <p><u>Attached Files</u>  Users can attach supporting documents to the submission. These documents are stored in their native format. For example, a Microsoft Word document will be stored in the COR file as a word document. It is assumed that the supporting documents are, by themselves, sufficient to understand the meaning of the documents.</p>
	<b>Supporting Documentation (list attachments):</b>
<b>18e. Ability to be viewed in human-readable format</b>	
	<b>Business Practices:</b>
	<p><b>System Functions:</b>  See Item 9b and 9c for more information on how the COR is provided in a human-readable format.</p>
	<b>Supporting Documentation (list attachments):</b>
<b>19. Timely availability of copy of record as needed</b>	
	<b>Business Practices:</b>
	<p><b>System Functions:</b>  MPCA-CROMERR generates the COR during the submission process. The COR is available for review using MPCA-CROMERR by registrants with the authority to view CORs for the specified organization, facility and CROMERR-compliant report. MPCA staff will also be able to view CORs. MPCA-CROMERR will allow users to search for CORs on at least the following fields:</p> <ol style="list-style-type: none"> <li>1. Submitter</li> <li>2. Permit ID</li> <li>3. Date Range</li> <li>4. Organization</li> </ol>

5. Facility

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

**Supporting Documentation (list attachments):**

**20. Maintenance of copy of record**

**Business Practices:**

**System Functions:**

CORs

MPCA-CROMERR CORs are stored/retained in the MPCA-CROMERR database, which resides on a database server. Submissions are stored in the database as a BLOB. A BLOB is a large block of data stored in a database and is a Binary Large Object. A BLOB has no structure that can be interpreted by the database management system, but is known only by its size and location. The use of BLOB is standard with database products when dealing with large data sizes. A document ID is associated with each COR BLOB. Each unique document ID is associated with a specific confirmation number. Each unique confirmation number is associated with a specific submission through MPCA-CROMERR. The CORs can be searched, viewed, and downloaded as specified in Item 19. MPCA-CROMERR will maintain CORs per the retention policy of the NPDES regulations and the MPCA. The COR will be maintained for at least 6 years from the date of submittal as required by CROMERR.

Logs

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

Database Backups

Physical Security

The MPCA-CROMERR application will be hosted on MPCA servers in the MPCA controlled access computer data center. The following reflect the procedures in place for this environment:

MPCA-CROMERR will be deployed in the MPCA secured Data Center environment. MPCA Data is backed up nightly which is rotated weekly to off-site storage under MPCA backup procedures and controls. Physical and environmental controls for the MPCA Data Center are provided, reviewed, and maintained by the CISO and Data Center Coordinator which include redundant AC, UPS, Fire suppression system, Card Access authorization procedures, environmental monitoring system, and emergency evacuation procedures..