

## CONTENTS

Exchange Network Leadership Council	1
Network Operations Board	1
Network Technology Group	6
Network Partnership and Resources Group	7
Drinking Water Integrated Project Team	8
Phase 2 Task Force	8

This summary details the month's activities of the Exchange Network Governance: Exchange Network Leadership Council (ENLC), Network Operations Board (NOB), Network Technology Group (NTG), and the Network Partnership and Resources Group (NPRG). It also contains information related to other Governance-sponsored activities this month (i.e., Integrated Project Team meetings, Task Force meetings, Open Calls, and Regional and National meetings). For more information on Exchange Network Governance, please visit: <http://www.exchangenetwork.net/about/network-management/>

## Exchange Network Leadership Council

The ENLC convenes a call every sixth Thursday from 3:00-4:30pm ET. There was no call scheduled in October.

*Next Call: November 1, 2012*

For more information on the ENLC, please visit: <http://www.exchangenetwork.net/about/network-management/exchange-network-leadership-council>.

## Network Operations Board

The NOB continues to focus on development of Virtual Node and Shared CROMERR Services technologies. The Virtual Node IPT convenes calls every other Tuesday from 12:00-1:30pm ET through the end of January. The Shared CROMERR Services IPT convenes calls every other Wednesday from 1:00-2:30pm ET through the end of February.

### October 2, 2012 – Virtual Node IPT Call

#### SUMMARY:

The October 2, 2012, call focused on four potential architecture models for the transaction construction pipeline. The main action item is the need to fully document the trade-offs for each architecture decision. The technical leads will work on this task with the Co-chairs and provide documentation to the IPT for discussion on the next call. IPT members are encouraged to email comments on these models to Kristen Durance (kdurance [at] rosstrategic.com)

The following comments and questions were highlighted by the IPT for each transaction construction pipeline model.

### *Model #1: "As-Is" View*

- New Hampshire does not allow outside connections from the DMZ to the operational data store. They would have to push data from the operational data store out to the DMZ to allow access.
- Gold Systems noted that for smaller programs like Tribes they use WQX web, which in essence acts like a junior virtual node. They do not have staging tables, but use flat files that are sent to EPA (like a node client). This set up is only used for data submission.
- Virginia has a slightly different picture. The State's node server sits in the DMZ and there is a firewall between it and the staging tables.
- Are architecture decisions driven by State requirements?
  - In Virginia, they are driven by requirements developed at the state level (i.e., no flexibility).
  - In New Hampshire, they follow state requirements, but organize their architecture in the manner that is most secure and logical for them. They may be able to make tweaks, but requirements are more or less absolute.

### *Model #2: Virtual Node Accesses Partner Staging Tables*

- Delaware does not allow anything from outside to go through a firewall. Outside resources cannot connect to the staging tables through the firewall in their architecture.
  - In this scenario, the Virtual Node would connect via a database protocol directly into the existing node staging tables.
  - The connection would be a dedicated connection, which means the node staging table would not be open to the internet (i.e., the connection is managed at the firewall).
  - Delaware could put another firewall on the other side of the staging tables that would allow access to the DMZ, but they are still not sure if their agency would allow direct connections to databases. Three-tiered architecture is the standard.
- Is there a reason not to put a public facing web service on the other side of the firewall?
  - The outbound connection would be managed via web service.
  - Could manage security with SSL or other protocols.
- The goal of the Virtual Node is to eliminate some of the partner-side components and lessen the burden that comes from managing local node instances. Partner nodes no longer exist with this model and it would allow Partners to move away from maintaining a node.
- The vision is not for a public facing database, but rather a connection via something like a VPN, which is probably allowable for many States. Connections would be dedicated, authenticated, and only from one IP to another.
- Data publishing aspects would only be allowed if they are configured by the data owner. SQL is not triggered by external requests, but by data owners' needs and schedule.
- The IPT does need to discuss the potential business cases where there is unknown type of request and the implications for managing those requests. What might be the anticipated uses and how that might affect architecture decisions?

### *Model #3: Virtual Node with Managed Staging Tables*

- Delaware thinks this is doable, but there is a concern about how truly sensitive data will be handled. Most data would be published.
- There were questions about where firewalls exist in the model. Jason described three separate networking zones with separate, physical firewalls:
  - Trading partner program systems and the operational data store;
  - Node staging table, Virtual Node, and firewalls protecting both; and
  - EPA receiving infrastructure.
- The Virtual Node is in a separate application stack and requests would traverse through the internet to communicate with CDX.
- Montana agreed that this diagram was much better for their system. The ability to push data out will simplify the process internally.

- Data could be pushed from the operational data store to the node in a bulk fashion (i.e., native format loaded into the virtual node format) or via native connections to the database (i.e., existing tools are pointed to new endpoints).
- Michigan noted they would require a VPN tunnel set up for this type of connections.
- Delaware noted that if they had the option to actually create an XML submission file internally and send that to the virtual node to be picked up and submitted they could reuse a lot of work already done internally (skip population of a full staging table).
- The technology can be “mixed and matched” to create a hybrid option from these models.

#### *Model #4: Virtual Node Accesses Program Database*

- The architecture using staging tables is not preferred by the trading Partners because it requires access to a data store (either the operational or a cloned version).
- This model allows more access to real-time data, but may also have the most barriers for State adoption.
- The key benefit is the removal of the staging tables from the Partners’ nodes. All functions are pushed to the virtual node. Changes in the schema or data flow will be accommodated by the virtual node and mapping to the staging tables is eliminated. Burden from a technical standpoint falls to EPA.
- Delaware noted that they did not think mapping on the virtual node could handle the more complicated flows correctly given how many data sources may be involved.
- Data owners may have issues with this model because data could appear on the internet without the QA/QC process currently done before sending data to EPA.
  - EPA clarified that there would be a testing environment on the virtual node where only the data owner could see the data. Data could also be secured with NAAS once in production.
- Montana would have to build staging tables exposing the operational data store or develop a clone for this model to work.
- If we consider this model from a data publishing perspective, how would it handle the data QA and data release?
  - The query is set in the virtual node and data would only be retrieved if it has been flagged for submission (e.g., it has been through QA/QC).
- Delaware noted that they do not publish much data.
- If you have to “approve” data, then the model is moving further away from real-time data, which is one of the big advantages of this architecture.
- A secondary copy of the data store does not necessarily have to affect the timeliness of data.
- Delaware would only push data from the operational to the clone data store on a set schedule.

#### **Questions for the Next Call**

- Are we optimizing the virtual node to satisfy the business process for data publishing, business process for national system reporting, or both?
- What are the pros and cons of each option and how do those affect what we are interested in optimizing?
- What are the tradeoffs between national system publishing and the goals of Phase 2?
- Which partners preferred Model #2 to Model #3? That could help identify the customers for the virtual node.

There was consensus that Model #2 offers the greatest flexibility and likelihood of partner adoption. The next phase of this conversation will involve understanding the tradeoffs for States, Territories, Tribes, and EPA, which will drive the ultimate decision.

*Next Call: November 13, 2012*

# October 31, 2012 – Shared CROMERR Services IPT Call

## SUMMARY:

### Grant Solicitation Materials

Products developed thus far from CROMERR IPT discussions are posted online at:

<http://www.epa.gov/exchangenetwork/grants/index.html>

### CROMERR Definitions Document

Will LaBar reviewed the CROMERR definitions document, which provides general descriptions of each service but does not include design specifics. The IPT has not yet reached that level of detail in discussions.

The following points were highlighted during the call:

- Most of the IPT came into the discussion expecting shared CROMERR services that invoke a web service.
- Trading Partners would interact with an interface that allows them to enter account information and credentials that are stored in the virtual CROMERR instance.
  - Challenge questions and answers would also be stored in the virtual instance.
- Most IPT members were expecting web services and not a UI. There were no concerns with using web services.

### Identity Proofing Discussion

The first topic for discussion was the basics of identity proofing including the use of electronic services currently available and wet ink signatures on Electronic Signature Agreements (ESAs). The goal was to highlight the types of services that could be provided via a shared service to help with ID proofing.

The following needs and considerations were identified:

- Password retrieval, reminders, resets (i.e., password management) are common due to the infrequency of data submission for some users.
- Some services require ESAs to be notarized when they are first submitted. How will this be handled in a shared environment?
  - This is not a hard requirement from CROMERR, but may be a State, Tribe, Territory or agency requirement.
  - EPA has phased out many of the services that used PKI and required a notary stamp because it is easier to automatically ID proof accounts.
- Connecticut noted that their Attorney General office requires companies to pass a corporate resolution to authorize the signature ability of staff for NPDES.
- How would proofing work for lower-level staff that may not get picked up in a LexisNexis® search?
- New York noted they have a system for ID proofing in place and are waiting to see how it interacts with the implemented shared service.
  - Pennsylvania also has a system in place and is unsure how it will connect. Probably will not have the ability to expose their database that houses account information because users are logging into the system via an Oracle web logic process.
  - Some States need the security managed locally. How would external system interface with those systems?
- Account maintenance will need more discussion as the IPT moves forward (e.g., name changes, staff turnover, link reminders, etc.).
- What are the costs associated with any third-party ID proofing options?
- Could the ID proofing system set up for shared CROMERR services be used for non-CROMERR services?
  - There are a number of similar programs that are not regulated through EPA, but rather the States and Tribes that have crossover with CROMERR.
  - Single sign-on (SSO) is a desire for many IPT members.

### *Account Creation*

Partners using a shared CROMERR service would invoke a web service that creates an account in a central repository.

- Partners that have their own centralized database may not be able to use this (e.g., Wisconsin, New York, and Pennsylvania)
- The service would require a feedback mechanism so that accounts are not created with similar names and emails (i.e., account validation and duplication checks).
- There are a number of fields required to create an account. This will need additional review.
- Authentication using multiple fields (e.g., is this email addressed used; ID taken; Password invalid) will require a lot of communication with EPA servers hosting the service. Need to keep this in mind when considering potential security risks like a hacker flooding the system with random emails and passwords. Instituting bot-blockers like CAPTCHA may be necessary. There are multiple options being explored for security.

Action: Work with FRS staff to see if there is crossover between the Facility IDs across programs to get a sense of how much overlap occurs. Will LaBar is following up.

### *Implementation Resource Requirements*

What are the returns if we go down a service implementation path that requires a lot of investment at the Partner level?

- There is an underlying assumption that every function a programmer does not have to write saves them time. So if the Partners' programmers do not have to write code and have it approved by their internal staff, then it saves them time. Calling on a function in the code will require programmers to develop the user interface that houses it but it is still a significant time savings.
- What about the resources necessary to link a central repository to non-CROMERR services?
  - Signatures are still required for these services at the State level.
  - The individuals submitting information may be the same as those submitting for CROMERR.
  - The level of "signature" may not be the same. In some cases it is just a check box next to a certification statement.
- A reasonable and higher standard makes sense. Do not want to create multiple standards for different regulatory processes.
- Passing Partner information on to a centralized service at EPA could cause privacy issues with some users. Need to define this in any user agreements.
- Users do not care if they are submitting to CROMERR or another system, but if the system is overly burdensome for a user who may only submit one permit then it would be problematic.
- EPA explored NIST standards. There are varying levels of stringency and many discussions around how much is necessary to provide assurance information is valid and safe. This is a future discussion topic.

### *Other comments*

- IPT may want to explore the option of giving authorizing contacts access to the account management panel (e.g., a manager at a larger organization). Multiple levels of access will be necessary.
- Account look-up function is available at the Partner level. If we centralize that database, then there could be privacy issues with other Partners being able to access personal information.
  - Some State Partners validate against their own DMV records. Would not want that accessible elsewhere.
- EPA does use LexisNexis® for ID proofing. Allows users to access public record information and other data shared by private companies. Provides a homogenized view of the data to consumer for data mining. They provide a set of ID proofing services that can be tailored to individual look-up needs.
  - Partners are interested in this option and potentially linking their own DMV databases.
  - EPA started using LexisNexis® because it allows multiple options and questions to be used to validate identity as required by Federal regulations.

## Discussion Topics for Next Call

- Continue discussions around account management.
- Use the summary findings from the questionnaire to highlight the account management requirements already identified.

*Next Call: November 14, 2012*

## Network Technology Group

The NTG convenes a call on the second Thursday of each month from 12:00-1:00pm ET.

### October 11, 2012

#### PARTICIPANTS:

Glen Carr (Co-Chair), Jason Payne, Phani Eturu, Kurt Rakouskas, Joe Carioti, Greg McNelly, Dennis Murphy, Yunhao Zhang, Tony Hartrich, Bill Rensmith, Doug Timms, Tony Jeng, Megan Parker, Rob Willis

#### ACTION ITEMS:

- Megan Parker will schedule the next REST Services subgroup call.
- Tony Jeng will document recommended language for the description field regarding what information would be useful for consumers of publishing services to incorporate into the REST and ENDS documentation and send to Kurt Rakouskas.
- Tony Jeng will examine the GLENDAs schema package to determine if there is a use case for having a new water quality flow without reusing the WQX schema and notify the NTG.

#### SUMMARY:

##### REST Services

- The REST Services subgroup is close to completing its work with potentially only one call left to finalize the documentation. After the documentation is finalized, the REST Services subgroup will submit it to the NTG.
- The NTG discussed enhancements to ENDS related to REST, including expanding the description field to make it easier for the data consumer to understand what kind of data they can expect from the data provider prior to the Query or Solicit. Another option would be to link to additional information on another site or the ENDS database; there is already a field in ENDS that could support this (service description field). This may require clarification in the ENDS FCD.

##### Schema Reviews

- Since the last NTG conference call, the ER3 and State Water Quality Assessment schema packages have been finalized and posted.
- The NTG sent comments on the GLENDAs package to the developers who made the requested changes. This package was resubmitted to the NTG via email and approved.
- The ICIS schema package was first discussed by the NTG on their last conference call with the action for Tony Jeng to review it and provide feedback to the group. After this review, the NTG received his comments and approved the package via email.
- The GLENDAs and ICIS schema packages will be posted.
- The TRIBES schema package was sent to the NTG. It has undergone two sets of reviews and developers have seen the most recent version.

- The NTG noted that the GLENDAS schema is intended to flow water quality data but is not reusing the WQX schema. There may be some business reason why the schema was not reused, and it would be good to identify this. There may also be a lack of communication about what schemas are available for reuse.

### Data Flow Conformance Review Process Changes

- On their monthly co-chair call, the NTG Co-Chairs discussed potential changes to the process for reviewing new and revised data flow packages. The goal is to reduce the burden from NTG members and provide more timely results to data flow developers when there are no critical issues to address.
- The following is the current data flow review process:
  - NTG Co-Chairs receive a data flow package for review.
  - ECOS or Ross Strategic sends the data flow package to the NTG and solicit volunteer reviewers.
  - ECOS solicits technical support contractor review through the ECOS/EPA Cooperative Agreement.
  - Technical Support contractors review and send their comments prior to the NTG call.
  - NTG members discuss the data flow package and the review on an NTG call where it is either approved or sent back to the flow developer to address remaining issues.
  - If approved, ECOS posts the package to the EN Website and sends an EN Alert.
- Depending on timing, the current review process can add several extra weeks to the review process in order to discuss reviews on the regularly scheduled NTG call.
- Most reviews are conducted by contractors and not by members of the NTG.
- The NTG Co-Chairs proposed altering the process so that it can move forward faster when reviewers have not found any critical issues that need to be addressed. This new data flow review process would be as follows:
  - NTG Co-Chairs receive a data flow package for review.
  - ECOS coordinates review by its technical support contractors.
  - Ross Strategic sends the schema package to the full NTG to notify members that the review is in progress. NTG members may participate in the review, but they are not expected to.
  - Reviewers will forward their comments directly to the flow developer, and provide a copy to the other reviewers, the NTG Co-Chairs, the Network Coordinator, ECOS, and Ross Strategic.
  - Flow developers respond to comments and resubmit any revised flow components to reviewers. If no significant issues remain, ECOS will post the package to the EN Website. This will eliminate the need for formal approval by the NTG.
  - If the data flow package still has significant or unresolved issues, then the Network Coordinator will work with the Co-Chairs to notify the NTG and forward the reviewer comments and the data flow package to the Group for discussion via email or on the next NTG call. The NTG will work with the flow developer to identify steps to address remaining issues, document any exception to EN design rules, or reject the package for posting to the EN Website.
  - After NTG approval, ECOS will post the data flow package to the EN Website and send an EN Alert.
- The changes to the process include only soliciting review from the contractor resources, reviewer comments being sent to the flow developers sooner, and posting the flow if there are no problems without NTG approval.
- The NTG agreed this new process will streamline schema package reviews, and to implement it.

*Next Call: November 8, 2012*

For more information on the NTG, please visit: <http://www.exchangenetwork.net/about/network-management/network-technology-group>.

## Network Partnership and Resources Group

The NPRG convenes a call on the first Thursday of each month from 2:30-4:00pm ET. The October 4, 2012, call was cancelled.

*Next Call: November 1, 2012*

For more information on the NPRG, please visit: <http://www.exchangenetwork.net/about/network-management/network-partnership-and-resources-group>.

## Drinking Water Integrated Project Team

The DW IPT is on hiatus until late January or early February 2013.

## Phase 2 Task Force

The Phase 2 Task Force convenes a call every other Tuesday from 2:00-3:30pm ET. The Task Force held one call in October.

### October 9, 2012

#### **PARTICIPANTS:**

Andy Putnam (Co-Chair), Jonathan Jacobson (Co-Chair), Mike Beaulac, Chuck Freeman, Chris Simmers, Greg McNelly, Lee Garrigan, Dennis Murphy, Joe Wilson, Rob Willis, Megan Parker

#### **ACTION ITEMS:**

- Kurt Rakouskas, Rob Willis, and Megan Parker will modify the governance structure diagram to reflect the Task Force discussion and create a written proposal for the ENLC and NOB Co-Chairs to review at their October 17-18 Meeting.
- Rakouskas, Willis, and Parker will make changes to the Phase 2 Implementation Plan based on comments received from the Task Force, including looking at the language around the Partner and Consumer definitions, and prepare a revised draft to send to the ENLC and NOB Co-Chairs prior to their October 17-18 Meeting.

#### **SUMMARY:**

##### **Governance Structure Reorganization**

- The Task Force discussed options for reorganizing the EN governance structure. A refined structure and diagram will be proposed to the ENLC and NOB Co-Chairs.

##### **Phase 2 Implementation Plan**

- Kurt Rakouskas reviewed the major changes to the document from the previous version and the Task Force provided comments.
- The ENLC and NOB Co-Chairs will review the Plan at their October 17-18 Meeting.

*Next Call: November 5, 2012*