Exchange Network Governance Activity Summary

November 2012

CONTENTS

Exchange Network Leadership Council	1
Network Operations Board	1
Network Technology Group	10
Network Partnership and Resources Group	10
Phase 2 Task Force	11

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.

The November 1, 2012, call was replaced by the November 15-16, 2012 ENLC Meeting held in Alexandria, Virginia. The Meeting summary will be posted to: http://www.exchangenetwork.net/about/network-management/exchange-network-leadership-council.

Next Call: January 24, 2013

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. The Shared CROMERR Services IPT convenes calls every other Wednesday from 1:00-2:30pm ET.

November 13, 2012 – Virtual Node IPT Call #6

ACTION ITEMS:

- CGI will continue to incorporate feedback provided by the IPT into the draft IPT recommendations document.

SUMMARY:

Security Discussion

VPN and SSH (Secure Shell) Connections

The IPT discussed the current use of VPN (CDX standard) and Secured Shell tunneling and how each could be used in a Virtual Node. The following comments were provided:

- Options will be deployed on a case-by-case basis to allow Partners to use technology that meets internal requirements.
- A VPN connection would be "always on" between the Partner agency staging servers and EPA.
- Security for the VPN connection would be firewall based with traffic only allowed between specific machines (i.e., machine-based, not user-based).

Role-based Security and Management

Based on the information gathered in the initial IPT survey there are three key requirements related to role-based security:

1. Different levels of node administrators (same rights as data flow administrators)
2. Managing access for End users
3. Screens to manage NAAS Accounts

End-user support will drive how this is developed. If we are trying to transition from node administration in the IT department to management at the program level then complete and easy to understand documentation will be necessary. Program staff will need to have final administrative authority within the Virtual Node. The IPT agreed that granular administration levels will be necessary for program staff to grant user access to the Virtual Node.

- New Hampshire noted that this is how they currently manage users. Program staff members manage access to their specific flow in the backend.

Other examples of role-based access activities that may require discreet roles include:

- Current roles will be necessary. For example, RCRA often requires programmers and program staff to work together to make changes and then re-run the data flow. This requires multiple roles.
- Possibility that a program office staff member may be modifying the SQL statements/mapping.
- Ability to configure the virtual mapping template or style sheet.
- Ability to trigger a flow that is not on a set schedule.
- Ability to view historical transactions for that data flow.
- Some users will require the ability to control the configuration of data flows. This will likely be a different person for each data flow, such as the data stewards.
- The Partner node admin should have the ability to make changes to any data flow within a state VN instance. Typically the program staff is savvy enough to know which data flows they should manipulate so this does not need to be managed on a flow-by-flow basis.

The IPT noted that it will be important to have someone knowledgeable available to trouble shoot (likely local IT staff) as it will not always be possible to rely on a central support structure to help.

User Management from a NAAS Perspective

The following features were discussed and highlighted:

- It would be great to have a UI to access and manage NAAS permissions as part of VN platform.
    - It is a little unclear if this would be the ability to create and modify accounts or just apply certain permissions.
    - There are a number of places where Virtual Node admin functions and NAAS admin function overlap.
    - CDX Web may be a better place to manage users as the Virtual Node was originally envisioned for business processes and not security management.
- From past experience, if we are trying to transition work to program staff and they have to go to multiple places to alter/create users then there will likely be push-back. We should be thinking about how to integrate all of these steps as much as possible.

- NAAS integration in Open Node includes the ability to create, delete, change, and reset passwords via web services. Organizations do this often if they want users to be able to access the node and Partners do create/delete users on a regular basis.
    - It has been confusing for some Partners to get the proper security via Open Node.
    - If we cannot interface to each flow, it would at least be helpful to have the access request routed to the right person at each program to make that process more fluid.

There are a lot of examples for historical national system flows. Are there any additional thoughts around user management needs for data publishing flows (e.g., an agency starting to publish incident/inspection/violation data that may need accounts set up for users to invoke the service calls.)? A two step security process might make sense: one open to the public and the other a NAAS registered account.

- All users must be authenticated before they can interact with the node and one work around for that is a generic account with a predefined password (e.g., public [at] epa.cdxnode.net).
- Other agencies have taken a similar approach: For example, the PNW Water Quality Exchange has a public website with NAAS credentials built in.

Change Management

The IPT discussed how the VN could percolate any changes that are implemented for a specific data flow on the VN. This would include changes to:

- Data flow (e.g., new schema that requires mapping changes and staging table updates)
    - Introduction of each change would need to be managed carefully.
- Changes to the node itself such as enhancements/upgrades to user interface

<u>Data Flow Changes</u>

- Each version of a data flow will be a separate instance and as changes occur, Partners can install a new version and maintain the old version (can move at your own pace).
- Hosting test and production environments with the ability to "promote" between the different environments will help reduce the level of effort required for each data flow.
    - Using a Copy/Clone environment could also leverage learning opportunities between Partners.
    - Developing a "template" might also allow the ability for anyone outside the national system flows to create a plug-in or template and share. This might require specific roles for those users.
    - Having the ability for a staff "testing role" that allows node admins to access the test server.
    - If outside users are allowed access a "sandbox" environment that would be helpful. This could provide access to the test/development environment in the cloud and not have to worry about those users accessing real data.
    - For some data flows we could shift from staging tables to reusable plug-ins, virtual mapping templates, or style sheets with transform information stored in the cloud for others to re-use.
- The idea of a schema "shelf life" was tabled for additional discussion in the future.

<u>Node Changes</u>

Changes to the UI and administrative screens within the Virtual Node will be handled with a "roll-out" process:

- Changes are suggested and Virtual Node users are given the opportunity to test the new capabilities in a test environment for a set period of time.
- Time would also be set aside for training on changes to the interface.
    - This training will be essential if we want program staff to be involved in the testing process.
- Roll-out would be set for a specific date once complete testing and review is complete. Ample notice will be provided for these types of changes.

<u>Other Types of Changes to Consider</u>

- MOU that lays out the notification process for changes, appropriate documentation, and scheduling along with the rules and expectations around version control for the base software.
- Core Node Specifications
- Governance needs such as how to manage release, and capture enhancement requests was tabled to next call.

November 27, 2012 – Virtual Node IPT Call #7

ACTIONS

- The VN IPT Co-chairs will look at the existing help desk relationships between EPA and the states to see if there is a way to make the general help desk inclusive of the Virtual Node

SUMMARY:

General Notes

The IPT had a brief review of the discussions from previous calls that have focused on Virtual Node "features" and what the centralized VN installation will do. The following points were highlighted:

Changes at the Data Flow Level

- Partners will implement a new flow when they are ready; not automatically pushed to each node instance. For example, if you have version 3.0 of the flow on your Virtual Node instance you would update to a new set of services when you are ready.
- The retirement of the old flow is handled through the existing EN Governance process.
- The IPT discussed how to make it easier for programs to manage their own data flows. Most programs do not have staff with SQL expertise, which is important for implementation of new flows. It might be helpful to have a list of "for-hire" contractors who can work with a centralized service to help with flow roll-out. There is a question of who is responsible for making changes to services held within the Virtual Node instance.
    - Some Partners are working on consolidating IT resources, which results in no IT expert on staff for individual programs. Centralizing the node and the resources needed to implement flows will help.
- Data flows are bound to a particular schema. When schemas change they change for everyone. The challenge will be in the mapping of schema to local data.
- If you are able to map to the node staging table then you are not likely to have to recreate the generation of payload. The hope is that if a program office makes a change to a dataflow they are also responsible for creating the linkage to the staging table.

Changes at the Feature Level

- The feature level includes items like the admin screens and navigation.
- When an enhancement is queued up (e.g., a new user interface for the administrative portion of the node) the change will be drafted with prior notification. Partners will have ample time, education, and training so that they fully understand any impacts to program office or node administrator. Full documentation will be developed and provided to implementing entities and then the change will be deployed on the Virtual Node.
- Timing for this process will be outlined in the draft recommendations for IPT reaction and comment.

Primitive/Service-Level Changes that are part of the Protocol and Specifications:

- This level applies to services like submit or query that are implemented by the Virtual Node.
- These services would only change when the Protocol and Specifications change according to existing mechanisms within the EN (e.g., through the ENLC).

Backwards Compatibility:

- There are some changes that could break existing data flows. Whenever changes are submitted they will be checked for compatibility with existing needs.
    - Most flows have supported one or two major changes to allow programs to move at their own pace. The only time this is not the case is when there is a new rule that requires updating.

The IPT agreed that these issues will be described in more detail in the Virtual Node IPT Recommendations Report.

- Data flow changes are controlled by the end user.
- Feature changes are managed by EPA.
- Node Specifications are handled by the existing process.
- Backward compatibility - will strive to use current practice.

Help Desk
The IPT discussed the need for a Virtual Node Help Desk and what type of support EPA and the Partners would be expected to provide. For example, an infrequent user may need guidance on how to configure the basics of a flow.

- Mapping will likely be maintained by staff on the Trading Partner side.
- Participants noted that program staff members are not the same as IT staff and that they may need quite a bit of support if they are expected to be responsible for flow changes.
    - It will be very important to fully document any configuration guidance.
- EPA noted that the Help Desk will be responsible for coordinating and helping users out at a fundamental level.
- It may be helpful to have a "for-hire" service that Partners could contract with for more advanced help. As long as that option remains available, then we probably have all possibilities covered.
    - The mapping process requires program expertise and it would be difficult to have someone drop in to do that work for a Partner.
    - It might be possible to use a current ECOS contractor to help Partners through the development process.
- The Help Desk should be available to Partners that need support for national system flow set up.
- A bulk of the hours set aside for the Help Desk will be for Partners to implement existing flows.
- The Help Desk should be able to answer fundamental questions about mapping (e.g., what is an FCD template), but there is programmatic knowledge that the EN Help Desk does not have. It would be a great step to establish better connectivity between the other help desk resources that are available via the EPA program offices.

Action: The Virtual Node IPT Co-chairs will look at the existing help desk to see if there is a way to make the general help desk inclusive of the Virtual Node.

The next Virtual Node call will focus on the initial draft recommendation document and the process for rolling that document out to a broader audience. The IPT will have a few weeks (over the holidays) to review the recommendations document in detail and provide comments prior to the January 8, 2013, call.

Next Call: December 18th, 2012

For more information on the Virtual Node IPT, please visit: http://www.exchangenetwork.net/about/network-management/network-operations-board

November 28, 2012 – Shared CROMERR Services IPT Call #5

ACTION ITEMS

- CGI will continue to incorporate the feedback from the IPT into the draft IPT recommendations document.

SUMMARY

General Notes
The IPT reviewed the topic schedule for the remaining calls. The IPT recommendations document drafting is scheduled to begin in January 2013. On the last call, the IPT discussed some of the identity management topics including "creating accounts". This call focused on the following ID Proofing topics:

- What shared services might look like through a third-party service
- Electronic agreement workflow for paper services
- Business affiliation proofing to meet CROMERR requirements
- Account approval and administrative services
    - For example, accounts are set up and noted as "pending" because there is a paper ESA to submit.
    - Delegation models. If and how an admin can query or see list of pending accounts and change to approve once required steps are completed.

The IPT was asked to share any specific questions or requirements they wanted to discuss related to the above topics and noted the following:

- Ability to use CROMERR signature services for state permits that may not be part of CROMERR (was noted as "single sign on" in past notes, but terminology was confusing). The end result is electronic signature gathering capability.
- How to plug in shared CROMERR services to current Partner applications. Will shared services interface with existing security systems?
- How will the pass back work to validate on both the virtual and Partner side?
- The ability to de-couple signature event from registration. Potentially with a local (or third party) ID (local account creation, ID proofing, etc.). Ability to use a local ID to complete the CROMERR signature event.
- Want to keep services agnostic to the ID service being used so that services remain pluggable.
- Trying to avoid having businesses being required to sign on twice (both local and CROMERR).
    - Need to examine on the accounts are set up at the state level and determine if registration for a state level credential includes a business process that provides ID proofing.
    - If you have trusted credentials that meet CROMERR minimums then you would establish a "trust" with EPA where the state is responsible for ID Proofing and only calls on the signature service from virtual CROMERR. This will depend on how security is set up in each state (case-by-case basis).
    - If the objective is that the signature and ID proofing are decoupled CROMERR would only require the signature ceremony and copy of record.

Identity Proofing Discussion

Individual ID Proofing

Identity proofing includes the process where a user creates an account, calls on a web service that then calls on a proofing service (e.g., the DMV). There are two potential workflows for this process:

- Account admin receives a notice and calls on a web service that communicates the authenticity of the credential to the shared CROMERR instance.
- ID proofing does not pass through the DMV check and is kicked to a second service (like LexisNexis). If that service is successful then the approved credential is passed on to the shared CROMERR instance.

Potential ID proofing services include state DMVs, SOS business list, tax records, VeriSign, and LexisNexis. EPA is currently using LexisNexis for CDX due to cost and available options that can be configured.

If the electronic ID proofing process completely fails or if the user "opts out" of electronic verification then the process moves on to a paper system where the user generates an electronic signature agreement (ESA) and mails it to the correct program office.

- The ESA content should be developed and managed by the individual states (there are some states that require AG approval of ESA text).
- The ESA is sent to local program staff members for approval. They create the account in the shared CROMERR services instance if the person passes proofing.
- We are assuming that the ESA goes to a local agency; they create an account in the shared CROMERR services, or create local credential and then use other SCSs.
- One state noted they were using a third-party service to verify identity of users. They charge a fee each time they are required to set up an account.
- The signature agreement has to be mailed somewhere and it seems like the data flow implementer would be the best contact. The state receives the ESA, validates, and then uses shared CROMERR services to approve the account.

Affiliation ID Proofing

EPA has found that electronic affiliation ID proofing is much more difficult that individual ID proofing. Some states are currently using the following methods to ID organization:

- New Hampshire: Some programs will call the organization, some require attestation form, some will check SOS, and others use an un-official source for affiliation proofing.
- Vermont: Mostly a manual process (nothing is formalized); some programs check SOS.
- Wisconsin: Uses an ESA and attestation form with each program managing this process differently.
- Oklahoma: Central solution, look up on facility profile then make a phone call.
- Connecticut: Looking for automated solution because they have so many different ways to do the proofing. Would also like to get an electronic verification from the system without having to wait for them to be completed.
- Pennsylvania: Looking at authorizing administrators.

Based on this information, it is assumed that Partners would continue to do what they have to do for affiliation proofing and then re-enter the shared CROMERR services workflow.

General comments:

- There is a lot implied if you are using Shared CROMERR for all account approval and admins will need the ability to query accounts based on status, view the listing, and impact the status using web services.
- An ESA is used for more than just signature verification. If a contractor takes on a new corporation then they would have to create a new ESA with the Partner program to have access to the new company.

Delegation Model

This model is set up so that a top tier official (e.g., the facility admin) is assigned a "responsible entity" role that allows them to manage the accounts for certifiers and preparers at their agency. This would require a UI for account management that would likely sit on each local system (rather than hosted in the cloud) so it would have the same look and feel as the state application.

- A certifier can sign a data submission, while the preparer is responsible for filling in all the required information.
- This may be overkill for small facilities/operators.
- Organization doing business in multiple states would likely need accounts in each state.
    - The IPT discussed the ability for shared CROMERR services to provide a single credential that could be used in multiple states. It is unclear how this would be set up and affiliated with the facilities.
- Each State can handle this process differently as long as web services are made available.
- Wisconsin, Michigan, New Jersey DEP, Mississippi, Massachusetts, New York, and Indiana currently have systems set up that support the delegated model. Wisconsin has found that there has been more turnover in responsible entity staff than anticipated.

Next Call Topics

- Wrap up the conversations around account data and authentication
- Discuss the details around the signing ceremony

November 28, 2012 – Shared CROMERR Services IPT Call #6

ACTION ITEMS

- CGI will review the specific legal requirements and indentify infrastructure options from the EPA side and provide those recommendations to the IPT. In general, there is interest in both developing a service and allowing States to continue process on their native application.

SUMMARY

Signature Ceremony

These services provide steps for verifying and validating the credentials of the user in order to apply a valid electronic signature to the CROMERR submission and produce the copy of record. The services include:

- Viewing the human readable copy of the submission. Make sure user knows what they are signing.
- Execute Ceremony
- Authenticate
- Retrieve info for ceremony
- Validate info during the ceremony
- Create/Apply
    - Signature EPA generates for CROMERR process is based on the XML digital signature standard. Hash is computed and a private/public key pair is developed

Human Readable Copy

The IPT discussed a few different implementation models for creating the human readable copy for review prior to electronic signature. There is an interest in both developing this as a shared service and leaving this to the Partners to deploy on their native application.

- There are many different application forms across the States. This may not be possible as a shared service.
    - Style sheet or PDF template that calls on the forms which is different for each form.
- How will the shared services get access to the readable copy if this is not deployed as a service?
    - Explicit parameter where the state sends the human readable copy to the signing ceremony service to apply the signature. At that time, the shared services become responsible for receiving, calculating the hash, and applying the signature.
    - We also need to discuss options for archiving the readable copy once sent to the shared service.
- Develop a service that bounces the human readable copy back with the hash first so that the order is: view doc, view has, sign, pass to final receipt (this way there is assurance that what the user reads is what gets sent to EPA).
- The hash is usually created when the document is created.
- Some of the forms we are talking about will never be submitted to EPA. For example, state requirements that need online forms. Only at the last stage where we have to validate the signature is when the shared services would come into play.
    - When we are talking about transmitting to EPA, it is only to call on the service for the signature ceremony and NOT to put the information in an EPA database. User is viewing what they are saying they are signing.
- There are a few places of vulnerability that need additional discussion:
    - Runtime service call submitted simultaneously
    - Admin capability: As they are provisioned for use the service manages the current version of the translation to generate the human readable copy.
- Participants noted that they would adopt a signature service even though they still have to go through the work of developing the style sheets because it still saves them time/effort.
- Partners would develop their own custom form to show to the end user for the signature process. A style sheet could only render an html page of the information and not the formatting particular to that Partner.
- Rendering of large payloads take a lot of resources. If service was high performance, then it would be a benefit.
    - Would rendering of large payloads need to be asynchronous?

Action: CGI will review the specific legal requirements and indentify infrastructure options from the EPA side and provide those recommendations to the IPT for review. In general, there is interest in both developing a service and allowing Partners to continue process on their native application.

Execute Ceremony

The signature ceremony seems to be a more “coupled” set of potential services that could be developed as one application rather than four stand alone services (retrieve, validate, authenticate, and create/apply). We may be able to

develop a widget that can be called to deal with all four of these steps and point to a customized data source that Partners have adopted (local, third party, or EPA).

The following questions were brought up:

- What level of flexibility is possible?
- Would multiple signatures for a single dataset be supported?
    - A document that requires a set of signatures for approval from different levels of staff at a company.
    - This could be handled as a stand-alone event where the second signature is applied to the copy of record, but if that is the case, they must be handled in a specific order.
- What is the workflow/order of events?
- Would this act like a web service or would we really be handing off the information to another application?
    - Would not hand off the information to an application hosted externally. It would be similar to Java Script where you inject specific elements into your native application.
- How do you get the certificate from the client without a widget?

Authenticate/Retrieve/Validate
A service would pass the user ID and password on to a central database and return a thumbs up/down on authentication. This is a straightforward process.

The 20-5-1 model is currently used for CROMERR services. Since those are available now, it gives us an immediate foundation to start with and existing resources that could be leveraged. But it is also not the most user-friendly model from an end-user standpoint. Partners are using the following methods:

- No second factor validation
- Challenge questions for password resets, which happen quite often.
- Considering moving the process to "out of band" via text message or email.
    - User sends a request and gets a code in their email all in one process.

Participants also noted that we will need good security measures in place to prevent malicious intent and that secondary verification to make sure a user is real might be necessary (e.g., CAPTCHA).

Create/Apply Signature
The service receives the human-readable copy and audit information, but we need to determine the output from that process. Do you get 20 COR if there are 20 separate documents? Some options include:

- An email is sent to the person who applies the signature with the COR, hash, and a printable PDF.
    - An out-of-band notification to verify signature that is sent from a "do not reply" email address.
    - This may need to be asynchronous.
- At the completion of the service, the user receives a transaction ID from which you could download the COR.
- Communication back to the initial application with the COR ID, transaction ID, and status (local application will show all of this) which communicates the success/failure.
- Audit Requirements: widget or service will need traceability

Next Call Topics

- Come back to the creation of the COR by the shared service and next steps.
- Position the IPT to develop the draft recommendations paper for review in January 2013.

Next Call: Wednesday, December 12, 2012.

For more information on the Shared CROMERR Services IPT, please visit:
http://www.exchangenetwork.net/about/network-management/network-operations-board

Network Technology Group

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

The November 8, 2012, NTG call was cancelled and instead used as time for the REST subgroup to meet.

Next Call: December 13, 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.

November 10, 2012

PARTICIPANTS:

Lauren Banks, Ken Blumberg, April Hathcoat, Jonathan Jacobson, Michael Kaufman, Heather Kenworthy, Jurgen Koch, Janice McLean, Greg McNelly, Jackie Moore, Kurt Rakouskas, Salena Reynolds, Chris Simmers, Virginia Thompson

ACTION ITEMS:

- NPRG members will contact Kurt with any comments or ideas to contribute to the changes in EN Governance.
- NPRG members will send any feedback they have on the Communications Plan to Salena Reynolds.

SUMMARY:

EN Governance Changes

- Kurt Rakouskas presented a summary of the ENLC's discussions about the Phase 2 Plan and the upcoming EN Governance changes that the ENLC would discuss at their November 15-16, 2012, Meeting.
- Jurgen noted that as Governance changes are taking place, it will be important to ensure that all current responsibilities of the existing groups are assigned to new groups or IPTs. Virginia echoed this concern, with particular regard for communications tasks. Kurt replied that communications will be a core, day-to-day staff responsibility.

E-Enterprise

- Ken Blumberg gave a presentation on E-Enterprise (formerly E-Reporting). The name could change.
- Enterprise is a still-forming concept, and represents a broader context within which the EN operates. The current conversation about E-Enterprise began over a year ago when an Executive Order was issued, and an effort to be consistent with the White House initiative on digital government. EPA's response to the Order was to review regulations and require E-Reporting where appropriate.
- E-Enterprise would, for example, allow a corporation that owns a facility to register with a central portal, identify themselves, what they do, where they do it, and they would receive information on what requirements they have in every State where they operate. This would reduce the burden on those companies.
- Grants to State and Tribal Partners would continue. The EN would continue to exist in the bigger vision of E-Enterprise, and is an integral part of the process. E-Enterprise can be built on some existing tools, including CDX, Virtual Node, and CROMERR-compliant web services.

- Tom Burack is co-leading a new ECOS-EPA workgroup with Andy Battin.
- There may be a way to integrate States' existing portals with the new central portal. The experience for the regulated entity would be transparent.
- The next steps for E-Reporting will be for four groups to convene. The first group will create a blueprint for the way forward, the second group will approach low-hanging fruit opportunities, the third group will serve as a governing body to work cooperatively with co-implementers, and the fourth group will handle communications.

EN Communications: CMR Presentation

- Jackie Moore and Lauren Banks of CMR presented a communications campaign implementation plan for the EN.
- Current steps include revising the EPA EN webpage to be consistent with, and not duplicative of, the EN website.
- CMR will develop a brand survey to reach out to non-technical audiences, will finalize a campaign umbrella message, and will incorporate a brand position statement into the existing EN logo.
- The NPRG discussed the scope of the communications campaign effort, and concerns that decisions are being made without input from EN Governance, particularly the ENLC. These conversations should be brought together in order to align with the new Phase 2 plan and the new direction of the Network.
- Kurt recommended that the ENLC should discuss the communications effort before this effort goes further, and that a new Communications IPT can provide input into the creation of any new communications and marketing plan. That process is how the new communications plan should be created.

Next Call: December 10, 2012

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

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 November.

November 5, 2012

PARTICIPANTS:

Andy Putnam (Co-Chair), Jonathan Jacobson (Co-Chair), Mike Beaulac, Chris Simmers, Kurt Rakouskas, Lee Garrigan, Greg McNelly, Ken Blumberg, Dwane Young, Rob Willis, Megan Parker

ACTION ITEMS:

- Kurt Rakouskas and Rob Willis will revise the Governance structure recommendations document and diagram based on comments from the Task Force and send to the ENLC prior to their November 15-16, 2012, Meeting.
- Dwane Young will talk to the Program Working Group Co-Chairs to determine how the group could better interact with the EN Governance structure and share this information with Kurt Rakouskas.
- Kurt Rakouskas will raise the question of how the Tribal Governance Group will interact with the new EN Governance structure at the ENLC Meeting.
- Phase 2 Task Force members will send any additional comments on the document or diagram to Kurt Rakouskas.

SUMMARY:

Exchange Network Governance Structure

- The Task Force revisited the recommendation for the revised EN Governance structure.

Next Call: December 4, 2012