Center for
Technology in Government

Exploring Regional Telecommunications Incident Response Coordination

Center for
Technology in Government

Exploring Regional Telecommunications Incident Response Coordination

Workshop Report

August 2007

Donna S. Canestraro
Theresa A. Pardo
Anna Raup-Kounovsky

Table of Contents

Executive Summary

In an increasingly interconnected world, neither the public nor the private sector can claim sole stewardship of the critical infrastructure. These interdependencies require new kinds of coordination in a variety of areas, particularly in response to incidents that threaten the stability of the critical infrastructure. Recent events such as the World Trade Center attacks and Hurricane Katrina have generated new discussions among stakeholders about the coordination necessary to ensure continuity of operation of the critical infrastructure. The federal advisory boards formed to review these events have cited the need for both stronger national as well as regional preparedness, while also noting a broad recommendation such as this must be tailored to meet the needs of specific regions. This is particularly the case for the telecommunications infrastructure which, while privately owned, is regulated by government. As a result, the federal government is focused on increasing response capability through increased coordination across sectors. Success in efforts at the national level together with encouragement from the telecommunications community have raised questions among states and localities as well as providers about the creation of regional coordination of telecommunications incident response as a complement to existing state and local level incident response capabilities.

In 2006 the New York State Department of Public Service (DPS), as a key actor in the national and regional telecommunications community, began to engage in discussions with other key actors about regional coordination of telecommunications incident response. Encouraged by interest from stakeholders, DPS partnered with the Center for Technology in Government (CTG) to organize a preliminary discussion among members of the regional telecommunications community. CTG brought together representatives of telecommunications providers, state emergency management agencies, federal communications agencies, state regulatory authorities, state departments of homeland security, state cybersecurity and the financial sector on March 28, 2007 for a one-day workshop. The workshop participants engaged in discussions about the value proposition of coordinated response capability, explored varying perspectives on the current state of affairs, brainstormed strategies for increasing regional response capability, and concluded the session by producing a set of conclusions about the current state of affairs and a set of recommendations for next steps in exploring regional coordination efforts.

The overriding value of a coordinated effort was identified as the continuity of government and the dominant strategy for achieving this continuity was recognized as securing access to real-time data to support informed decision making across each of the four stakeholder groups; government, the providers, the private sector and citizens. Workshop participants agreed that the telecommunications community needs to invest in public trust and demonstrate their ability to keep functioning in a time of crisis. From the telecommunications provider viewpoint, securing the telecommunications infrastructure and providing rapid and cost effective incident response was considered a matter of stewardship – “stewardship of the network, the organization, and the confidence of the citizens and regulators that providers will be able to restore service in the most efficient and effective manner possible. The challenges to these efforts come from both physical barriers to obtaining credentialing to gain access to restore services and the limited capability to share time sensitive information.” Participants agreed greater coordination is key to overcoming these challenges.

Overall, participants agreed that regional coordination of telecommunications incident response should continue to be explored as a strategy for ensuring continuity. One participant noted, “It’s intuitive that it’s a good idea to do this. Sharing information will help us respond better.” However, participants recognized the importance of a detailed and thorough exploration of the idea. Clarity of purpose and value were considered paramount. In the words of one participant, “Continue to clarify what you’re trying to accomplish because if there’s a good, compelling reason, there should be lots of support.” Regardless of the specifics of the exploration, participants called for full representation of stakeholders in the process, clarification of roles and responsibilities both in terms of leading and participating in the exploration itself and in the strategies for regional coordination considered as part of the exploration. Participants agreed the greatest challenge to any multi-organizational collaboration is in the creation of a governance

structure. The exploration would therefore need to generate insights on strategies and best practices in this area.

Five recommendations emerged from the discussions to guide the exploration. The participants urged that, first and foremost, management principles for the coordination study should be jointly developed by a multi-sector group and these principles, once established, should be used to guide the implementation of the additional recommendations. The second and third recommendations address the issue of knowledge gaps. Each participant had knowledge of their own organization, but recognized the lack of sufficient knowledge and opportunity to collectively identify processes and practices and to look for optimization and coordination opportunities across organizations. The fourth recommends an investment in analysis of the current flow of information to determine performance criteria and areas for improvement. Finally, participants recommended that DPS and others continue to seek support and funding for this exploration through state, regional, federal and private sources.

Recommendation # 1 Jointly establish guiding principles
Bring together the key actors from across the sectors to collaboratively establish guiding principles to steer continued work in this area. For example, the principle of "collect once – use many times," if widely adopted, might result in more information sharing across organizations.

Recommendation # 2 Conduct current practice research
Current and best practice research regarding regional coordination of infrastructure incident response must be completed. The research should specifically focus on regional coordination of telecommunications incident response, as well as models for the governance and information sharing agreements of existing regional response efforts.

Recommendation # 3 Increase knowledge about current information resources, practices and capabilities
Regional coordination should not duplicate response capabilities in either the public or private sectors; this was very strongly communicated by stakeholders both before and during the workshop. However, it became evident throughout these discussions that the current knowledge of all parties did not provide a full picture of what currently exists. Without this knowledge it is impossible to assess if there are in fact duplicative efforts. Participants recommended that each of the primary stakeholders perform an assessment of their own organizations' informational needs and resources, as well as their capability to share information across organizational boundaries, to determine what information they will be willing to share with the larger community.

Recommendation # 4 Invest in process improvements
A number of the participants stated before and during the workshop that any future efforts should provide value to all stakeholders in order for them to participate. One way to identify value was to look at the current flow of information to determine if there was in fact a better way for information to be shared. The concept of collect once – use multiple times became a common theme in these discussions. The information flow models need to be developed through collaborative group model building sessions to allow for shared understanding. Analysis of these models will inform decision making about process improvements, if needed. This effort will also provide the opportunity to increase the capability of telecommunications incident response by providing collaborators with additional knowledge that may not have been available before. Through this process it may be found that these improvements may or may not include regional coordination.

Recommendation # 5 Secure funding for continued exploration
A comprehensive study of the potential value of a regional coordination effort will require new resources. The cost of this effort will exist primarily in coordinating the serious and consistent involvement of the many stakeholders necessary to ensure representative and well-informed recommendations are produced. Funding sources, such as state and federal emergency and homeland security agencies, should be contacted for possible interest in funding this effort both as an investment in capability in the northeast region and as a model process for other regions throughout the States.

A number of conclusions emerged from the discussion regarding the current state of affairs and are put forward below as additional guidance in implementing the five recommendations.

Knowledge gaps exist - A key finding from the workshop is that, regardless of future investments in regional coordination, the gap in current knowledge about the roles and responsibilities of individual organizations in sub-national incidents needs to be addressed. In addition, the knowledge of who has what information at any point in time that could be brought to bear on incident response is unclear.

Roles and responsibilities are unclear – Participants were unclear about who is responsible at what point in time in the event of an incident. This lack of clarity about responsibility, or "who is in charge" at the regional level, echoes findings in the President's National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the National Coordinating Center (May 10, 2006), which was used as background for this project.

Currently held information resources can be leveraged - Regional incident response requires leveraging currently held information resources in innovative and potentially more efficient ways, as well as the establishment of new business processes, communication flows, and a system of governance that satisfies the needs of all stakeholders.

Trust and collaboration are pivotal - Trust, collaboration, and timely cross-boundary information sharing play a pivotal role in this coordinated response. Trust is built when government partners and telecommunications providers are able to work collaboratively to restore service in a cost effective and efficient manner. This type of collaboration creates conditions that allow for continuity of government, which in turn builds citizen's trust in government.

Quality and timely data - Receiving detailed information quickly becomes especially important in regional, multi-state, or multi-jurisdictional responses. Real-time data and cross-organizational information sharing are even more significant in the smaller, localized events where only one critical infrastructure is involved. A telecommunications incident response can be severely hindered if the response team lacks quality and timely data. Having knowledgeable workers as near to the "ground" as possible and having access to a "clearinghouse" for information were identified as being two important aspects of increasing response capability.

Contextual knowledge matters - Contextual knowledge of the region is imperative for decisions concerning resource distribution, response time estimates, and deployment of special equipment in response to an incident. Sharing information alone will not help refine the response; knowing what information was important within the context of where the incident occurred and what items are needed for restoration of service was viewed as being equally valuable as the sharing itself.

National Communications System (NCS) may provide a model - The NCS roles and responsibilities as documented through the NRP is one example of information sharing and disaster management model in the event of a national incident (further details about the NCS and other regional collaboration models are located in Appendix 3 Current Practice Review). The question remains, however, to what extent might a similar model be relevant when an incident was localized to either a specific geographic area or jurisdiction beneath the federal radar?

Introduction

In an increasingly interconnected world, neither the public nor the private sector can claim sole stewardship for a stable critical infrastructure. These interconnections create a complicated web of priorities and responsibilities. This is particularly the case for the telecommunications infrastructure that, while wholly privately owned, is regulated by government. New interdependencies require new kinds of coordination of efforts in a variety of areas, in particular in the coordination of response to events which threaten the stability of the critical infrastructure. Many federal advisory boards have cited the need for both stronger national and regional preparedness, while also noting a broad recommendation such as this must be tailored to meet the needs of specific regions. Recent events such as the World Trade Center attacks and Hurricane Katrina have generated new discussions among stakeholders about the coordination necessary to ensure response capability. As a result, a number of initiatives at the federal level have focused on increasing coordination capability across sectors in terms of response to national incidents. Successes in these efforts at the national level together with encouragement from the federal advisory boards have raised questions among states and localities as well as providers about the creation of sub-national regional approaches to telecommunications incidents as a complement to existing state and local level incident response capabilities.

In 2006 the New York State Department of Public Service, (DPS) as a key actor in the national and regional telecommunications community, began to engage in discussions with other key actors in the region about launching an exploration of regional coordination of telecommunications incident response. Encouraged by interest from stakeholders, DPS partnered with the Center for Technology in Government (CTG) to organize a preliminary discussion about this idea among members of the telecommunications community. CTG brought together representatives of telecommunications and financial providers, state emergency management agencies, federal communications agencies, state regulatory authorities, state departments of homeland security, and representatives from state cybersecurity on March 28, 2007 for a one-day workshop to focused on this idea.

The stakeholders engaged in discussions about the potential value of regional coordination through the use of CTG's Public Value Framework, exploring how such coordination might deliver value to various stakeholder groups. A key aspect of this discussion was concern about unnecessary duplication of effort and that regional coordination should not duplicate response capabilities in either the public or private sectors. Participants at the workshop agreed that regional incident response requires leveraging currently held resources in innovative and potentially more efficient ways, as well as the establishment of new business processes, communication flows, and a system of governance that satisfies the needs of all stakeholders. In addition, trust, collaboration, and timely cross-boundary information sharing all play a pivotal role in this new model. A key finding from the workshop is that, regardless of future investments in regional coordination, the gap in current knowledge about the roles and responsibilities of individual organizations in sub-national incidents and the understanding of who has what information at any point in time that could be brought to bear on incident response need to be clarified.

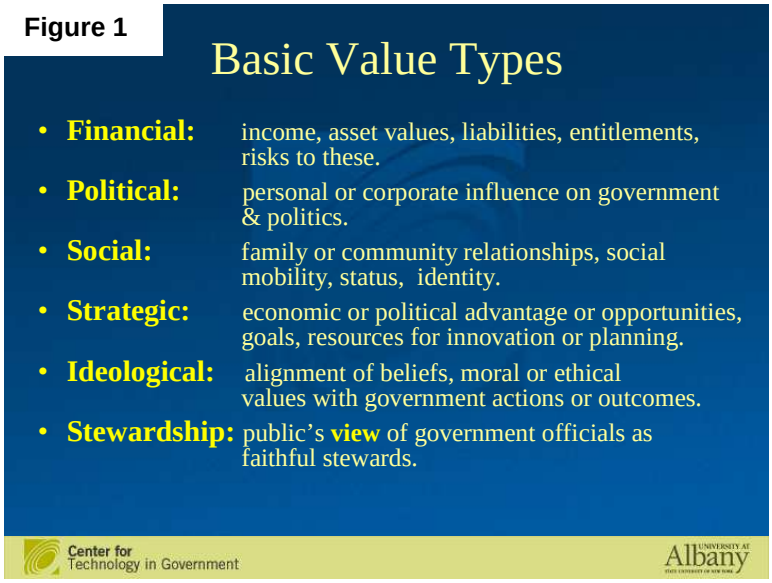
This report summarizes the workshop discussions and includes a set of recommendations from the participants for next steps in exploring regional response coordination. The report outlines how the value of coordination was assessed by workshop participants and presents their prioritization of perceived benefits of and challenges to regional coordination. Suggestions for how this report might be used to assist in moving the discussion forward within and across each of the various sectors are also provided.

Assessing the value of a regional telecommunications response

Due to the focus of concern around the added value of new regional coordination capability, CTG asked the participants to consider how value is generated in general. Expanding the traditional Return on Investments (ROI) methodology beyond mere dollars and cents, CTG asked participants to consider the current and ideal telecommunication incident response efforts from six different value types[1] : financial, political, social, strategic, ideological, and stewardship These values types are based on the idea that government generates value to its constituents in two ways:

- By improving the ***value of the government itself*** from the perspective of the citizens, and
- By delivering ***specific benefits directly to persons, groups, or the public at large***.

Figure 1



The first is based on the idea that, assuming a benign government, the better it functions overall, the better off its citizens will be. The government is an asset to the community or nation that delivers a wide range of values. Internal improvements make it a more valuable asset to the public. The second way of generating value has three forms: financial, political, and social. Financial value results from lowering the cost or increasing the efficiency of government or delivering direct financial benefits to the citizens. Political value consists of increasing participation, fairness, transparency, legitimacy, or conferring political capital to elected officials or citizens. Social returns include increased social status, stronger relationships, or opportunities; increased safety, trust in government, and economic advantage. (See Figure 1). This framework proposes that value can be realized through the increase in efficiency, the increase in effectiveness, enablement of otherwise infeasible or prohibited activity, and intrinsic enhancements to the stakeholder. The following section outlines how this value framework was used in the workshop discussions.

Public value by stakeholder

Using the six value types, (Financial, Political, Social, Strategic, Ideological, and Stewardship), participants were asked to consider the value an ideal telecommunications incident response system would provide to four key stakeholder groups (Citizens, Telecommunications Providers, Government Sector, and the Private Sector). In a collaborative process guided by a facilitator, the group discussed the current challenges preventing them from achieving this ideal state. The participants discussed the impact the value proposition has for each of the value types by key stakeholder group. The following provides a brief synopsis of the key elements within each (refer to Table 1 for a complete listing of the responses.)

Citizen

Participants discussed the importance of maintaining citizen trust in government and in telecommunications providers. They agreed that trust is built when citizens see government and providers working collaboratively to restore service in a cost effective and efficient manner. The

[1] Refer to: Advancing Return on Investment Analysis for Government IT: A Public Value Framework http://www.ctg.albany.edu/publications/reports/advancing_roi

group agreed that better information sharing would result in better decision making on the part of both the providers and government officials, the consequence of which would be greater continuity of government, increased public trust, and decreased duplication of efforts. As one participant stated, "The more information the carrier has in assessing the incident, the quicker they can restore service. It is a financial issue to citizens – it all comes down to rates." Citizens, the participant noted, "see decreases in cost as being evidence of better government."

Telecommunications Providers

From the telecommunications providers' viewpoint, the importance of information sharing and cooperation across sectors took on a different perspective. It became a matter of stewardship – stewardship of the network, the organization, and the confidence of the citizens and regulators that providers will be able to restore service in the most efficient and effective manner possible. The challenge to this was not only the barrier to obtain credentialing for access to restore service, but also the capability to share information that is time sensitive. As one participant stated, "[From the provider's perspective,] there is an underlying contract with customers to restore services as quickly as possible. The number one priority during a disaster is to get business back to normal." However, another provider stated, "The challenge is [that] the people helping to put the information together are likely to be the same people working on the network." All participants agreed that an expedient way to restore normal operations is through collaboration and sharing of real time data at the level of detail required to successfully remediate an incident.

Government

Representatives from the government sector spoke both in terms of telecommunications incident response and emergency management. One participant stated, "Since Hurricane Katrina, we've totally changed the way we think." The participants discussed incident response from a national level and all agreed that the National Response Plan (NRP), National Coordinating Center for Telecommunications (NCC), a part of the National Communication System (NCS), and Department of Homeland Security (DHS) have a structured model for public/private partnerships. All agreed that the physical co-location and the sharing of information that occurs during weekly meetings at the NCS with the private and public sectors benefits all concerned.

All participants agreed on the need to avoid duplicating existing services. Various participants had the perception that data was already being shared from the federal level down to the state/local level. However, based on further discussion among the participants, it became apparent that this was an assumption that had never been fully tested. One state official used the analogy that "there is this pond up there, where information is shared back and forth at the federal level, but the lower level where state and local areas are situated – there is not the real-time access to this information. If there is a crisis in Albany, it may not rise to the NCC until a week or two weeks later and we can't wait for the synthesis of this data. The mayor of Buffalo, NY or the governor wants to know much more about the impact in real time. They can't come out of the meeting feeling like they do not know everything to alleviate public concern."

Private Sector

The private sector participants noted additional challenges due to the cost of ensuring continuity of service in the event of a telecommunications incident. In the private sector, corporations must fulfill their stewardship responsibilities to their investors. Participants also discussed issues related to an organization's ability to provide contingency plans in the event of a service disruption. As one participant stated, "The information is key to knowing if you need to make an investment in plan B. If you don't have adequate reliability, you make the decision to invest in back-up carriers." All concurred that, like government, private sector organizations need to invest in public trust and demonstrate their ability to keep functioning in a time of crisis.

Overall, the value proposition that most resonated with participants was the importance of continuity of government and the ability to have real-time data to support informed decision making across each of the four stakeholder groups. The discussion then segued into the characteristics of the ideal response from a national, regional (state), or local response. The next section provides an overview of these discussions.

Table 1.
Exploring Public Value by Key Stakeholder Group

Value Type	*Key Stakeholder Groups*			
	Citizen	**Telecom Provider**	**Government Sector**	**Private Sector**
Financial	• Potential of improved service • Less down time or interrupted services • Continuity of Government	• Dissemination of information resulting in system reliability and continuous investment in infrastructure • Critical resource restoration • Avoidance of misappropriation of funds • Cost sharing across providers • Less regulatory risk of penalties	• Continuity of Government • Better use of taxpayers funds – creation of a clearing house • Better able to coordinate response efforts to avoid waste of time, resources, and finances.	• Continuity of service allowing rates to be maintained • Pass along savings to citizenship. • Ability to plan and attend to needs of customer base • Responsiveness
Political	• Improve or maintain trust in government and providers Continuity of Government	• Political with a small p –information sharing between providers and government allows for trust to be earned by the regulators • Enhanced relationship between providers and government • Potential gains in public trust • Provides or exhibits capability allowing for increases in public trust, confidence, and continuity of service	• Increases in confidences in providers • A show of stability to all sectors • Allows for better service to leadership through information sharing	• Perception of government as vigilant and on top of things • Less rate increases
Social	• Well informed, confident in government's ability to take care of infrastructure • Good will • Increase in public confidence • Increase in expectations • Ability to know that service will be restored in a timely fashion • Reduction in chaos and fear	• Increase in good will • Increase perception of the public of the service providers provide • Increase in perception of responsiveness and collaboration among providers in a time of crisis	• Increase or maintain credibility • Continuity of service • Increase in public confidence	• Employee relations and confidence in employer and in government. • Less impact to service and ability for employees to maintain productivity. • Less frustration on the part of workers
Ideological	• Good Government	• Market demands being met	• Responsiveness to citizenship • Continuity of Government	
Strategic	• Increase in security	• Quick informed decision making • Sound decision making based on just in time data	• Better ability to plan • Sound decision making based on just in time data • Better gap analysis	• Better position for recovery • Ability to have contingency plans that are based on good information
Stewardship	• Trust • Increased public confidence in government • Continuity of service	• Provides evidence of corporate stewardship	• Improved infrastructure investments • More informed regulation • Better decision making	

Current environment

In the event of a national disaster

As the workshop participants worked together to clarify how telecommunications incident response management occurs in the event of a national disaster, the group agreed that the National Response Plan (NRP) would go into effect and guide their actions Under the NRP, the NCC, a part of the NCS, coordinates information sharing to the Joint Field Offices (JFO) and the State Emergency Management Offices (SEMO). For example, in a national disaster, such as Hurricane Katrina, JFO and SEMO worked together to collect and coordinate information from a variety of critical infrastructure sectors; telecommunications information would only be one area about which data is collected. The mechanism for collecting and disseminating information for all critical infrastructure (CI) sectors is dictated by the NRP. The NCS, working with colleagues in both public and private sectors, keeps the President and all necessary individuals posted regarding the response and restoration activities.

The workshop participants agreed that the roles and responsibilities as documented through the NRP provide a model for information sharing and disaster management in the event of a national incident (further details about the national and other regional collaboration models are located in Appendix 3 Current Practice Review.) The question remains, however, to what extent might a similar model be relevant when an incident was localized to either a specific geographic area or jurisdiction beneath the federal radar?

In the event of a state or regional disaster

The participants agreed that in the event of a local, regional, or state disaster, the NCS may not receive detailed information about the incident or play a role in the response. According to NCS officials, the NCS watch center tracks those local events that catch their attention; however, they are only alerted or called into action when an event is identified as threatening an asset related to national security or emergency preparedness (NSEP) In the event of a regional or localized telecommunications incident, the NCS may not mobilize their members or mobilize only for information purposes; therefore information may not be disseminated by the NCS to the many different local entities that cross the organizational sectors.

Below the national or state radar

As the participants revealed these important distinctions in the nature of disasters of both national and non-national interest, they pushed their conversation further to examine the information flows and the roles and responsibilities of various organizations from national, state, regional and local levels. Many of the workshop participants raised concerns about roles, responsibilities, and non-duplication of services. Less clear to the participants was who is responsible at what point in time in the event of an incident. This lack of clarity about responsibility, or “who is in charge” at the regional level, echoes findings in the President’s National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the National Coordinating Center (May 10, 2006), which was used as background for this project.

In the event of a national or state-wide emergency, the National Response Plan (NRP) and the State Emergency Response Plan (SERP) are called into effect; however, in regional or local incident response, according to the participants, there is currently no coordinated information sharing plan. In the absence of a cohesive, regional information-sharing plan there is the potential for duplication of information and increased complexity in the coordination of various actors.

A key point highlighted by the participants is that real-time data and cross-organizational information sharing are even more significant in the smaller, localized events where only one critical infrastructure is involved. Participants noted that certain local events may fall under the radar of even a regional coordination effort. However, they identified the importance of keeping the appropriate government officials informed so they can reassure and advise the public in a time of crisis.

Importance of data and contextual knowledge

Participants repeatedly emphasized the value of accurate, sufficient data and contextual information sharing in a time-sensitive environment; receiving detailed information quickly becomes especially important in regional, multi-state, or multi-jurisdictional responses. A telecommunications incident response can be severely hindered if the response team lacks this granularity of data along with the contextual knowledge of

the region. As an example of the value of contextual knowledge, one of the participants discussed the potential for underestimation of regional implications of an event. "If, say a telecommunications call center in Dallas, Texas became aware that electric service was down in the Palisades cliff area of New Jersey, it might not appreciate the potential impact to telecommunications in that region. Regionally remote call centers would likely have limited knowledge about what that service outage means to the local service technicians in a geographic area such as the cliffs of the Palisades, a 550-foot-high precipice along the west bank of the Hudson River in Bergen County, New Jersey and Rockland County, New York. The call center attendee, without knowledge of this geographic area, might not fully appreciate the logistical challenge of this response, nor the implications for telecommunications services in NYC, Westchester, and Northern New Jersey."

In one participant's view, this type of regional knowledge is imperative for decisions concerning resource distribution, response time estimates, and supplying special equipment in response to an incident. Participants stressed the importance of having knowledgeable workers as near to the 'ground' as possible. Creating a "clearinghouse" for information was another important aspect of improving both the quality of the data and the speed with which it could be delivered. Sharing information alone would not help refine the response; knowing what information was important within the context of where the incident occurred and what items are needed for restoration of service was viewed as being equally valuable as the sharing itself. This focus on local expertise is also consistent with the National Response Plan's view that "the lowest jurisdictional level" possible should provide incident response.[2] Accomplishing this vision effectively means responders will need timely, accurate information.

Investigating Alternatives

The workshop concluded with a focus on how the current environment could be changed to increase the public value provided by telecommunications incident response. Participants considered this question from a local and regional perspective. The participants also considered if any of these alternatives warranted further investigation.

Responses fell into three specific categories of activities:

Clarifying or Establish Guiding Principles –The participants discussed the principle of "collect once – use many times" as being a mantra that should be followed in incident response. All agreed there are likely multiple information collection activities being conducted across the various sectors. The format and reporting structure may vary based on information's origin and owner. But the main principles that initiated this investigation (that there may be a better, more cost effective way to share information and the importance of the public/private partnership) continued to be true. The participants stressed the importance of developing guiding principles to help steer continued work in this area.

Conduct Current Practice Research – These activities focus on producing inventories of systems, repositories, data stores, and best practices reviews. In addition to the identification of the information resources currently available, it was noted that the owners of these resources and the rules that govern these resources should also be documented. The importance of the identification of roles and current responsibilities was also noted as a critical step in testing assumptions that there is already a structure in place providing regional coordinated telecommunications incident response.

Invest in Process Improvement – All agreed there were many ways to improve on what was currently being done, while also making the point that future efforts should not 'tinker with something that isn't broken'. The activities identified as ripe for process improvements could be considered current practices.

[2] "A basic premise of the NRP is that incidents are generally handled at the lowest jurisdictional level possible. Police, fire, public health and medical, emergency management, and other personnel are responsible for incident management at the local level. In some instances, a Federal agency in the local area may act as a first responder and may provide direction or assistance consistent with its specific statutory authorities and responsibilities. In the vast majority of incidents, State and local resources and interstate mutual aid normally provide the first line of emergency response and incident management support." (National Response Plan, page 15.)

Rather than reinvent the telecommunications response, participants suggested analyzing what was currently being done to look for inefficiencies.

Table 2. Activities by Category
Guiding Principles
Identify clear expectations (roles and responsibilities) of carriers and government.
Improve public awareness of response mechanism.
Create an environment to increase and maintain trust among the participants.
Clarify a process in which the regional centers and individual state procedures co-exist and are well-understood.
Establish the uses to which collected information would be used and retain awareness of confidentiality issues.
Ensure interoperable critical infrastructures.
Provide training and dissemination of information to trusted partners on infrastructure and local knowledge.
Create a forum where local and regional entities can discuss and share issues.
Create an information sharing template so information shared and the process for sharing is consistent.
Current Practice Research
Identify relevant models (NCS, ISAC, NIPP, NYS DPS, NYS CSCIC and the like).
Identify interdependencies outside of sector.
Clarify potential value of regional approach for multiple events.
Investigate various methods for alerts – such as the Web, hand-held devices, etc.
Clarify roles of existing repositories & decide whether and how best to create regional center without duplication
Identify in all sectors day-to-day activities that add value.
Create a common set of credentialing criteria and process.
Define a region.
Define what information is shared and with whom, and under what conditions.
Create a data inventory – not only of the data but also of the rules governing the data and ownership.
Process Improvements
Establish a protocol for an authoritative source for providing public info.
Conduct a vulnerability assessment and address the gaps in existing arrangements.
Create mutual aid agreements.
Explore possibilities of FOIA and the dissemination of info.
Identify the barriers to information access.
Formalize informal contacts and create a standard personnel list.
Create a governance structure.
Create a GIS or contextual layer to the data gathered.

Once the list of activities was generated, participants were asked to vote on the initiatives they considered to be of high priority and those they considered to be highly do-able (refer to the appendices for a complete listing). Table 3 lists the top two initiatives selected for each of these categories.

Both private and public sector participants ranked “Create a governance structure” as the highest priority but as one of the least do-able activities. All acknowledged that creating this structure would be difficult because of the challenge of creating these bodies across organizational boundaries and among multiple, potentially competing partners. However, participants also noted that although creating this in a collaborative way would be challenging, it is the only way it could work. It should not be mandated by any regulatory or government entity. Participants noted that all participating groups need to see the value in forming a governance structure in order to gain buy-in and succeed in creating the governance structure.

Table 3. Investments in Effort
High Priority
• Create a governance structure
• Identify clear expectations (roles and responsibilities) of carriers and government
High Do-ability
• Clarify roles of existing repositories & decide whether and how best to create regional center without duplication
• Establish a protocol for an authoritative source for providing public info

Participants were asked to consider the value likely to be generated by the creation of a governance structure and the identification of clear expectations from the four areas where value could be realized: increases in efficiency, increases in effectiveness, enablement, and intrinsic enrichment—for the 4 key stakeholder groups. Working in two small groups, the participants came to similar conclusions about the potential value of pursuing the top four initiatives, as well as what would need to change for that value to be realized. Table 4 lists what needs to happen for that value to be realized and Table 5 lists the specific value participants identified that each stakeholder group might expect from successful investments in the top four initiatives.

Both discussions highlighted the challenge and complexity these efforts will involve from policy, organizational and technological perspectives. The participants felt the establishment of the governance structure and the clarification of roles and responsibilities would help mitigate many of these challenges.

Table 4. What must change for the value of a regional coordinated telecommunications incident response to be realized?
1. Establish a threat or incident threshold that indicates when to activate a regional response
2. Establish an agreement about the need for a regional response
3. Decide a clear focus for what might become the “region” and who needs to participate
4. Solve conflicts with authority by reducing turf arguments and protectionism
5. Not too much other than to bring together existing lists and protocols
6. Nothing- just better organization and bring together the current lists and protocols
7. Better communication and cross-sector sharing of information
8. Meet with stakeholder groups to establish protocols
9. Meet face to face and work through state or federal government legislative chair
10. Must be willing to work across jurisdiction lines and must give up need to control
11. Open dialogue between agencies to understand what each has to offer
12. Structure and document roles in information sharing
13. Commitment to voluntarily agreement on a model/structure
14. Clarify responsibilities of the state/federal/private participants

Table 5. Value to Stakeholder Groups				
	Citizens at Large	***Telecom. Providers***	***Government Sector***	***Private Sector***
Increases in efficiency	• Better use of taxpayer money • Faster response time during a telecommunications incident • Provide a single source for the public to get accurate information	• Decrease the burden of reporting • Single source for direct information • Clarify roles and responsibilities • Increased ability to respond to a telecommunications incident • Better able to develop cross-sector partnerships.	• Increase transparency and facilitate greater trust • Enhance existing partnerships and develop new ones • Streamline costs to support the response process	• Better awareness of where to go for information • Forum to address critical infrastructure needs
Increases in effectiveness	• Higher quality information	• Reduce burdensome reporting requirements • Clearly established protocols for incident response • Better control of information • More effective response to an outage • Clarify roles and responsibilities	• Potential to receive better information faster • Clarify roles and responsibilities • Better management of resources • Allow agencies to focus on their own specialties	
Enablement		• Build trust with government • Higher level of accountability • Better information at a lower cost	• Increase trust and partnerships with other sectors • Better information at a lower cost	• Higher degree of accountability
Intrinsic Enrichment	• Better coordinated regional response to disasters • More orderly response to telecommunications incidents	• Able to be more responsive to a telecommunications incident	• Better organized response structure	• Gain confidence from telecommunications providers and government

Key Conclusions

Table 6 summarizes the key conclusions generated from the workshop. Overall, participants agreed that regional coordination of telecommunications incident response should continue to be explored. One participant noted, "it's intuitive that it's a good idea to do this. Sharing information will help us respond better." However, participants recognized the importance of a detailed and thorough exploration of the idea. Clarity of purpose and value were considered paramount. In the words of one participant, "Continue to clarify what you're trying to accomplish because if there's a good, compelling reason, there should be lots of support." These conclusions represent a starting point for this effort. Regardless of the specifics of the approach chosen, participants called for full representation of stakeholders in the process and clarification of roles and responsibilities, both in terms of leading and participating in the exploration itself and in the strategies for regional coordination considered as part of the exploration. Participants agreed the greatest challenge to any multi-organizational collaboration is in the creation of a governance structure. The exploration would therefore need to provide insights on strategies and best practices in this area. Another key element identified by participants is the documentation of current as well as ideal communication and information sharing channels and encouraged workshop organizers to prepare a report of the workshop both as a record of the discussion and as a tool to seek support and funding for the continued exploration. Finally, participants encouraged the key stakeholders to continue to move this process forward through the creation of a report of the workshop and through the use of the report and companion pieces to secure support and funding for the required exploratory study.

Table 6. **Key Conclusions**
Current Environment
• All agreed NCP and NCS are models for disaster management in the event of a national incident.
• Of shared concern is when an incident is localized to either a specific geographic area or jurisdictions beneath the federal radar.
• In the event of a regional or localized telecommunications incident, the NCS may not mobilize their members or mobilize only for information purposes; therefore, information may not be disseminated to the many different local entities that cross the organizational sectors.
• Real time cross-organizational information sharing is even more important in the smaller, localized events where only one critical infrastructure is involved.
Value to the Public
• The potential value created through enhanced coordination capability that resonated with the participants is continuity of government and real-time data to support informed decision making across each of the four stakeholder groups.
• In the event of a regional, multi-state or multi-jurisdictional response, the participants emphasized the need to receive detailed information quickly so appropriate government officials are kept informed and can reassure and advise the public in a time of crisis.
• Both government and private sector organizations need to invest in public trust and demonstrate capability to function in a crisis.
Information Sharing in Context
• A telecommunications incident response can be severely hindered if the response team lacks granularity of data and contextual knowledge of the region.
• Regional knowledge is imperative for decisions concerning resource distribution, response time estimates, and supplying special equipment in response to an incident.
• Participants stressed the importance of having knowledgeable workers as near to the ground as possible.
• Creating a clearinghouse for information is a potential strategy for improving the granularity of the data and the speed with which it could be delivered.
• Knowing what information is important within the context of an incident is equally important to sharing.
Do not duplicate or tinker with something that is not broken
• Do not duplicate existing services at the state or regional level.
• Improve on what is currently being done while being sure not to tinker with something that isn't broken.
• Explore all possibilities and test all assumptions.

Recommendations

The five recommendations workshop participants put forward are presented below. The participants urged that, first and foremost, management principles for the coordination study should be jointly developed by a multi-sector group and that these principles, once established, should be used to guide the implementation of the additional recommendations. The second and third recommendations address the issue of knowledge gaps. Each participant had knowledge of their own organization, but recognized the lack of sufficient knowledge and opportunity to collectively identify processes and practices and to look for optimization and coordination opportunities across organizations. The fourth recommends an investment in process analysis of the current flow of information to determine performance criteria and areas for improvement. Finally, the participants recommended that DPS and others continue to seek support and funding for this exploration through state, regional and federal sources.

Recommendation # 1 Jointly establish guiding principles
Bring together the key actors from across the sectors to collaboratively establish guiding principles to steer continued work in this area. For example, the principle of "collect once – use many times," if widely adopted, might result in more information sharing across organizations.

Recommendation # 2 Conduct current practice research
Current and best practice research regarding regional coordination of infrastructure incident response must be completed. The research should specifically focus on regional coordination of telecommunications incident response, as well as models for the governance and information sharing agreements of existing regional response efforts.

Recommendation # 3 Increase knowledge about current information resources, practices and capabilities
Regional coordination should not duplicate response capabilities in either the public or private sectors; this was very strongly communicated by stakeholders both before and during the workshop. However, it became evident throughout these discussions that the current knowledge of all parties did not provide a full picture of what currently exists. Without this knowledge it is impossible to assess if there are in fact duplicative efforts. Participants recommended that each of the primary stakeholders perform an assessment of their own organizations' informational needs and resources, as well as their capability to share information across organizational boundaries, to determine what information they will be willing to share with the larger community.

Recommendation # 4 Invest in process improvements
A number of the participants stated before and during the workshop that any future efforts should provide value to all stakeholders in order for them to participate. One way to identify value was to look at the current flow of information to determine if there was in fact a better way for information to be shared. The concept of collect once – use multiple times became a common theme in these discussions. The information flow models need to be developed through collaborative group model building sessions to allow for shared understanding. Analysis of these models will inform decision making about process improvements, if needed. This effort will also provide the opportunity to increase the capability of telecommunications incident response by providing collaborators with additional knowledge that may not have been available before. Through this process it may be found that these improvements may or may not include regional coordination.

Recommendation # 5 Secure funding for continued exploration
A comprehensive study of the potential value of a regional coordination effort will require new resources. The cost of this effort will exist primarily in coordinating the serious and consistent involvement of the many stakeholders necessary to ensure representative and well-informed recommendations are produced. Funding sources, such as state and federal emergency and homeland security agencies, should be contacted for possible interest in funding this effort both as an investment in capability in the northeast region and as a model process for other regions throughout the States.

A number of conclusions emerged from the discussion regarding the current state of affairs and are put forward below as additional guidance in implementing the five recommendations.

Knowledge gaps exist - A key finding from the workshop is that, regardless of future investments in regional coordination, the gap in current knowledge about the roles and responsibilities of individual organizations in sub-national incidents needs to be addressed. In addition, the knowledge of who has what information at any point in time that could be brought to bear on incident response is unclear.

Roles and responsibilities are unclear – Participants were unclear about who is responsible at what point in time in the event of an incident. This lack of clarity about responsibility, or "who is in charge" at the regional level, echoes findings in the President's National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the National Coordinating Center (May 10, 2006), which was used as background for this project.

Currently held information resources can be leveraged - Regional incident response requires leveraging currently held information resources in innovative and potentially more efficient ways, as well as the establishment of new business processes, communication flows, and a system of governance that satisfies the needs of all stakeholders.

Trust and collaboration are pivotal - Trust, collaboration, and timely cross-boundary information sharing play a pivotal role in this coordinated response. Trust is built when government partners and telecommunications providers are able to work collaboratively to restore service in a cost effective and efficient manner. This type of collaboration creates conditions that allow for continuity of government, which in turn builds citizen's trust in government.

Quality and timely data - Receiving detailed information quickly becomes especially important in regional, multi-state, or multi-jurisdictional responses. Real-time data and cross-organizational information sharing are even more significant in the smaller, localized events where only one critical infrastructure is involved. A telecommunications incident response can be severely hindered if the response team lacks quality and timely data. Having knowledgeable workers as near to the "ground" as possible and having access to a "clearinghouse" for information were identified as being two important aspects of increasing response capability.

Contextual knowledge matters - Contextual knowledge of the region is imperative for decisions concerning resource distribution, response time estimates, and deployment of special equipment in response to an incident. Sharing information alone will not help refine the response; knowing what information was important within the context of where the incident occurred and what items are needed for restoration of service was viewed as being equally valuable as the sharing itself.

National Communications System (NCS) may provide a model - The NCS roles and responsibilities as documented through the NRP is one example of information sharing and disaster management model in the event of a national incident (further details about the NCS and other regional collaboration models are located in Appendix 3 Current Practice Review). The question remains, however, to what extent might a similar model be relevant when an incident was localized to either a specific geographic area or jurisdiction beneath the federal radar?

Appendices

1 Workshop Participants
2 High Priority/Hi-Do-ability Matrix
3 Current Practice Review

Appendix 1. Workshop Participants

Telecommunications Incident Response Exploratory Workshop

March 28, 2007
Albany, NY

Mary E. Burgess, Esq.
AT&T Communications of NY, Inc.
meburgess@att.com
Phone: 703-607-4922

Victor DeVito
Area Manager, Regulatory Relations
AT&T Communications
vdevito@att.com
Phone: 908-234-4374

Andrew Feeney
First Deputy Director
Emergency Management Office
State of New York
andrew.feeney@semo.state.ny.us
Phone: 518-292-2305

Douglas Frazier
Energy Policy Advisor
Office of Homeland Security
State of New York
dfrazier@security.state.ny.us
Phone: 518-408-1100

John Gibb
Director
Emergency Management Office
State of New York
John.Gibb@semo.state.ny.us
Phone: 518-292-2227

Garnet Goins
Director, State Regulatory Affairs
Sprint Nextel Corporation
garnet.goins@sprint.com
Phone: 703-433-4248

William Johnson
Assistant Deputiy Direct and CIO
Office of Cyber Security and Critical Infrastructure Coordination
State of New York
william.johnson@cscic.state.ny.us
518-474-0865

Dakin Lecakes
Assistant Counsel
Department of Public Service
State of New York
dakin_lecakes@dps.state.ny.us
Phone: 518-474-4536

Peter Pescosolido
Chief of Regulation for Telecommunications
Department of Public Utility Control
State of Connecticut
peter.pescosolido@po.state.ct.us
Phone: 860-827-2802

Timothy Peterson
Chief of Staff
Public Safety and Homeland Security Bureau
Federal Communications Commission
Timothy.Peterson@fcc.gov
Phone: 202-418-1575

Dennis Taratus
Chief, Network Reliability
Office of Telecommunications
Department of Public Service
State of New York
dennis_taratus@dps.state.ny.us
Phone: 518-486-5649

Brian S. Tishuk
Executive Director
ChicagoFIRST
brian.tishuk@chicagofirst.org
Phone: 312-992-0603

Workshop Coordinators/Facilitators
Center for Technology in Government

Donna S. Canestraro
Program Manager
dcanestr@ctg.albany.edu

Anna Raup-Kounovsky
Program Staff Assistant
arkounovsky@ctg.albany.edu

Theresa A. Pardo
Deputy Director
tpardo@ctg.albany.edu

Appendix 2. High Priority/High Do-Ability Matrix

3/28/2007 Workshop Results
Exercise 2

Initiative	High Priority Votes	Highly Doable Votes
1. Training on infrastructure and local knowledge		
2. Local knowledge culture		
3. Strategy of ramp up on local knowledge		
4. Awareness of interdependencies outside of sector		Total = 3
5. Clarify potential value of regional approach for multiple events	Total = 2	
6. Explore possibilities of FOIA- Dissemination of info	Total = 4	
7. Environment to increase trust	Total = 2	Total = 1
8. Formalize informal contacts and create a standard personnel list	Total = 5	Total = 6
9. Mutual aid agreements	Total = 2	
10. Mutual assistance among various telecom – working together		Total = 1
11. Regional telecom response plan under the NIPP	Total = 4	
12. Connect regional efforts among levels of government	Total = 3	Total = 2
13. Clarify roles of existing repositories & decide whether and how best to create regional center without duplication	Total = 5	Total = 7
14. Common set of credentialing criteria and process- cards	Total = 5	Total = 4
15. Governance- how will this operate	Total = 7	
16. Identify day-to-day activities that add value in all sectors	Total = 1	Total = 1
17. Data inventory: who reports what to whom- and why?	Total = 1	
18. Find out what constricts our ability to get info we need? Fill knowledge gaps		
19. Clear expectation of carriers and government—everyone needs to know his/her role	Total = 7	Total = 3
20. Establish a protocol for an authoritative source for providing public info	Total = 1	Total = 7
21. Use of the Web as a tool for alerts on service disruption	Total = 1	Total = 5
22. Regional forum for commons approach for issues (creating SOPs, etc.)	Total = 3	Total = 1
23. Clarify a process in which the regional centers and individual state procedures co-exist and are well-understood by all	Total = 3	Total = 2
24. Vulnerability assessment- gaps in existing arrangements	Total = 3	Total = 3
25. Establishing the uses to which collected info would be used- retain awareness of confidentiality issues	Total = 4	Total = 5
26. Make public aware of actual response		
27. Define what a region includes		Total = 5
28. Define what info is shared and with whom	Total = 1	Total = 1
29. Info sharing template so info is consistent and have way to put it into a GIS so we can have in context with other info	Total = 4	Total = 4
30. Making sure other critical infrastructures can interface between other critical infrastructures	Total = 1	Total = 2

Appendix 3. Current Practice Review

Summary

As part of the background research on regional partnerships, the Center for Technology in Government conducted a brief review of several U.S. and Canadian models of regional collaboration and crisis management. Overall, we found that many types of organizations are currently striving to form stronger intergovernmental and cross-sector collaborations as part of their strategies for more robust incident response, both in telecommunications and in other areas of critical infrastructure. The summaries below offer some initial observations about these organizations with a focus on regional collaboration. As recommended by the workshop participants, a more in-depth review of current practices is necessary as part of any effort launched to further explore the feasibility and advisability of regional coordination of telecommunications incident response.

National Coordinating Center for Telecommunications (NCC)

Since 1984, the National Coordinating Center for Telecommunications has been responsible for ensuring the reliability and continuity of the national telecommunications infrastructure. As of 2000, the NCC also serves as the Information Sharing Analysis Center (ISAC) for the Federal Government.

In order to effectively develop national security/emergency preparedness (NS/EP) capabilities, the NCC relies upon a formalized membership structure. Under the supervision of the NCS, the NCC is run by both the Manager and the Deputy Manager who oversee all NCC operations. With the support of a dedicated staff, the Manager works with both resident representatives, who are co-located at the NCC Watch Center, and nonresident representatives, who act as liaisons between their organization and the NCC. Industry and government participation are vital to the NCC and their representation is decided by established criteria, which includes the organization's degree of involvement in NS/EP activities, its status as a communications asset, and its Federal Emergency Management Agency (FEMA) designation.

During a national crisis, the NCC takes the lead in the restoration of telecommunications, with a focus on previously identified personnel who are integral to the recovery effort. Industry representatives are responsible for providing incident reports to the Manager, who then supervises the dissemination of that information to relevant government agencies. However, the NCC is more than a crisis response center. Normal daily activities include developing response plans and sharing information about potential threats and vulnerabilities to the national assets within the telecommunications infrastructure.

To support this goal, the NCC offers additional federal recovery response programs designed to assist both the private and public sector organizations involved in telecommunications, including the Government Emergency Telecommunications Service (GETS), an emergency communication service used when normal lines of communication are severed; Shared Resources (SHARES), which provides voluntary transmission of emergency messages; and the Telecommunications Service Priority (TSP), which prioritizes agencies that need rapid restoration of services in the event of a telecommunications incident.

www.ncs.gov/ncc

ChicagoFIRST

ChicagoFIRST is a non-profit organization that represents Chicago's financial institutions and collaborates with city, state, and federal agencies to ensure continuity of operations and the safety of their employees in the event of a crisis. When the majority of major cities across the U.S. began strengthening their disaster plans after the World Trade Center attacks, Chicago's financial institutions became concerned about their own ability to respond to a disaster. This concern led to the formation of

ChicagoFIRST, which works to secure the city's financial resources and to maintain financial services even during a crisis. Although ChicagoFIRST grew from private sector interests, they quickly began working with strategic partners from the public sector, including the City of Chicago, the State of Illinois, the U.S. Treasury Department and the Department of Homeland Security.

ChicagoFIRST has seen many successes in crossing the divide between private sector business continuity plans and public sector disaster management. Membership from the financial sector has grown from 14 to 25 institutions, and there are now 26 strategic partners from the public sector and nonprofit organizations.

ChicagoFIRST has gained respect for its success in coordinating private sector efforts in business continuity with public sector and non-profit organizations' disaster planning. In December of 2004, the Treasury Department released a case study and handbook based upon the ChicagoFIRST model, titled *Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions*[3]. As an organization, ChicagoFIRST has also taken on an active role in encouraging financial partnerships throughout the country. To support new regional partnerships, ChicagoFIRST has been instrumental in establishing RPC*first*, a collective of financial business networks based upon the ChicagoFIRST model. RPC*first* brings together the leaders from both emerging and established financial services partnerships to share knowledge about disaster planning, as well as providing a direct line of communication to the federal government through the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).

www.chicagofirst.org

King County Regional Public Information Network

The Regional Public Information Network (RPIN) is a Web-based alert system hosted by King County in Washington State. With support from the American Red Cross, RPIN was established in 2000 to provide the public with a one-stop resource for information about health, transportation, and emergency response. Membership in RPIN is free and voluntary, although agencies are asked to commit to security, content accuracy, and outreach on behalf of the network.

Although network agencies are encouraged to collaborate, there are no formal governance structures to guide cross-sector collaboration. During normal operations, member agencies provide information as they deem necessary; during a crisis, agencies continue to control their own information, but they work through a regional joint information center (RJIC) to provide more coordinated announcements to the public.

RPIN is mainly a one-way communication resource for the public. Although anyone can access the RPIN announcements through the Web site, citizens can also create free membership profiles. With a subscription to RPIN, they will receive emails with relevant safety alerts, which they can then tailor to their specific needs or interests. Announcements can be filtered by county (King, Pierce, or Snohomish County) and by the alert category (Emergency Alerts, or widespread emergencies; Transportation Alerts, including road closures and transit service disruptions; and Other News, which covers all other bulletins and disruptions).

www.rpin.org

Pacific Northwest Economic Region (PNWER)

PNWER is a public-private partnership committed to promoting economic growth in the Northwest while sustaining the region's natural resources and environment. Established in 1991 through coordinated

[3] http://www.ustreas.gov/press/releases/reports/chicagofirst_handbook.pdf

legislation in the member states and provinces, PNWER has representatives from Alaska, Idaho, Montana, Oregon, Washington, British Columbia, Alberta, and the Yukon Territory.

PNWER relies upon a well-established governance structure to manage the elected representatives and private sector partners who form its membership; the organizational chart below outlines the main councils and committees. The Delegate Council is the founding body of PNWER, and therefore takes on the role of aligning the organizations' current activities with its original mission and goals.

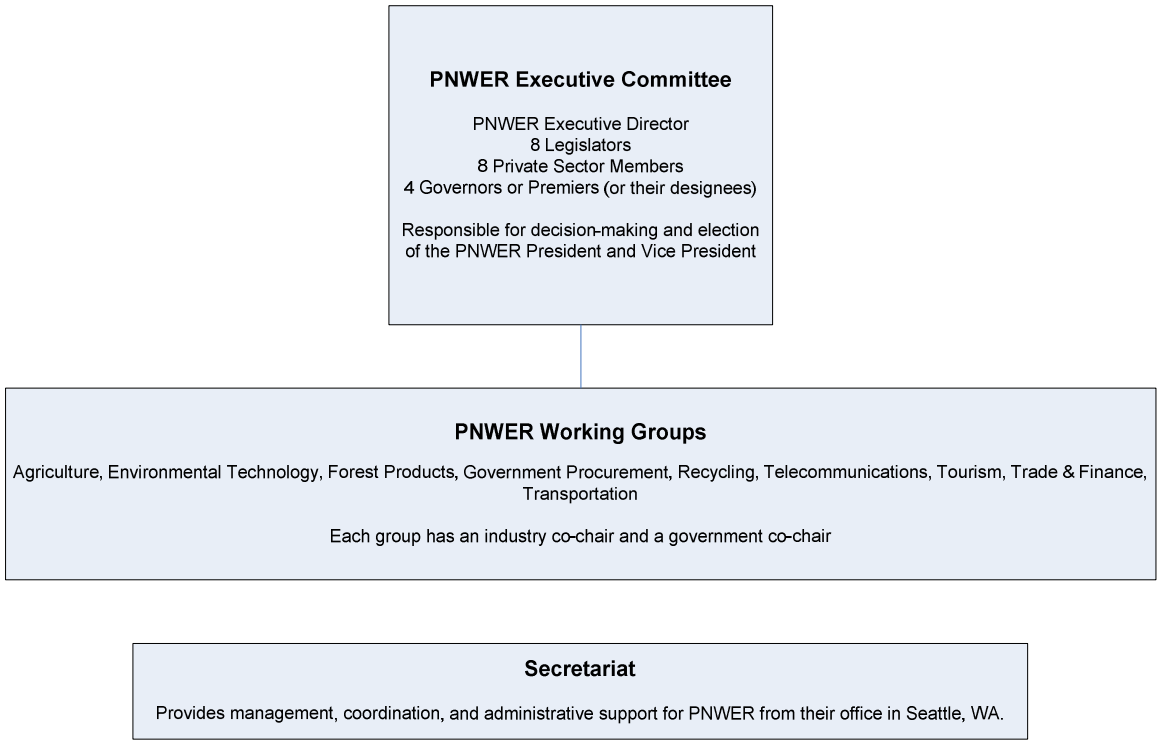


Figure 1. PNWER Organizational Chart[4]

In order to reach its goal of sustainable economic development, PNWER has nine working groups to focus on specific areas of interest: Agriculture, Environmental Technology, Forest Products, Government Procurement, Recycling, Telecommunications, Tourism, Trade & Finance, and Transportation. Each of the working groups regularly reports their activities to the Executive Committee. PNWER's Annual Summit provides a forum for all of the Working Groups to hold their meetings and enables face-to-face information sharing and collaboration among the various PNWER members.

www.pnwer.org

New Jersey Regional Operations Intelligence Center (ROIC)

With a new facility at the State Police headquarters, New Jersey's Regional Operations Intelligence Center (ROIC) is already improving law enforcement in the state. Described as a "fusion center," the ROIC provides a single reporting site for three information sets: law enforcement intelligence, public

[4] Source: http://www.pnwer.org/AboutUs/Background/Organization/tabid/65/Default.aspx

safety, and private sector reporting. The Center also has three main goals as it moves forward: inclusiveness, regionalization, and transparency.

The ROIC is still in its early stages of development as a regional center for law enforcement data. However, it has already developed strong partnerships with a variety of public safety agencies. Run by the New Jersey Department of Homeland Security and Preparedness, the Center also houses the Office of Emergency Management and the state Emergency Operations Center (EOC). The ROIC also receives regular input from the FBI, the US Department of Homeland Security, FEMA, the NYPD, bordering State Police, a range of New Jersey state agencies, local county and municipal governments, and many non-government partners.

Center for Technology in Government
182 Wolf Road, Suite 301
Albany, NY 12205
Phone: (518) 442-3892
Fax: (518) 442-3886
E-mail: info@ctg.albany.edu
www.ctg.albany.edu

UNIVERSITY AT ALBANY
State University of New York