



Pacific NorthWest Economic Region

1

Testimony

**Matt Morrison
Executive Director
Pacific NorthWest Economic Region (PNWER)**

May 25, 2007

**U.S. House of Representatives
Committee on Homeland Security**

**Subcommittee on Intelligence, Information Sharing,
and Terrorism Risk Assessment**

Seattle Field Hearing entitled:

**“Building a Partnership Strategy: Improving Information Sharing with State
& Local Law Enforcement and the Private Sector**

**Bellevue City Council Chambers
Bellevue City Hall
450 110th Ave NE
Bellevue, WA 98009**

May 25, 2007

**US Congressman Bennie Thompson
Chairman
Committee on Homeland Security**

Mr. Chairman and Members of the Committee,

I commend you for the title of today's Seattle Field Hearing: "Building a Partnership Strategy: Improving Information Sharing with State & Local Law Enforcement and the Private Sector"

This is exactly the right topic to be addressing as it cuts to the centerpiece of how this nation needs to be and can be better prepared to face the wide range of natural and man-made hazards with a comprehensive system of systems approach to preparedness and the mitigation of vulnerabilities in our communities.

Since 9-11 there has been a great deal of focus on physical protection, and infrastructure sector specific plans. As we all saw this week, Secretary Chertoff announced the Sector Reports under the National Infrastructure Protection Plan have finally been released.

While it has been a positive step to increase the security of our infrastructures to terrorist attacks, as we saw with Hurricane Katrina, there is a pressing need to focus on cross-sector cooperation, coordination and information sharing to achieve regional disaster resilience. As yet, DHS has not focused in any meaningful way on cross-sector challenges to the all-important task of building regional resilience. Infrastructures and essential service providers in a region are tightly interdependent and subject to cascading failures that can incapacitate entire communities. What this means is that a utility or other service provider may have the best security possible and still have its operations or business practices damaged or disrupted.

Resilient regions are able to bounce back from any kind of disaster with limited impacts on public health and safety, the economy, and national security. If we want to have 'Resilience' from either a natural hazards or a terrorist attack we must be able to understand the vulnerabilities caused by regional interdependencies, what assets and facilities are truly critical, and determine cost-effective ways based on risk to prevent or mitigate these vulnerabilities. The only way to gain this understanding is through cross-sector partnerships that foster local trust among all the key stakeholders that have roles or vested interests in providing critical products and services or which have emergency preparedness and management responsibilities. This is a large number of organizations—all levels of government, private sector, non-profits, academic and research organizations and community institutions.

What I have just described is what we call the 'Resilience Tautology'. To state it simply,

- Resilient assets and infrastructures require resilient regions
- Resiliency requires understanding which assets are critical in any specific scenario

- Understanding criticality depends upon understanding the interdependencies between and among critical infrastructures (85% of which are privately owned). Criticality is dynamic and changes during an incident, often in unanticipated ways
- Interdependencies remain undiscovered in stove-piped sector specific planning
- Understanding interdependencies require cross sector information sharing
- Cross sector and public/private information sharing requires the creation of an environment of trust where stakeholders feel ‘safe’ to share their vulnerabilities with each other and with first responders and government

To emphasize, comprehensive planning for resiliency cannot be done without having all the key stakeholders together – sharing in a trusted environment – which provides a value added resource to each and all of them. Regional Resilience requires that procedures and protocols for information sharing be worked out in advance of any incident, and that stakeholders work together to mitigate vulnerabilities and address shortfalls in a consistent framework within a public private partnership. This process cannot be done by the government or the private sector alone, but only in a trusted partnership with all key stakeholders in a community.

PNWER’s Long Role in Fostering Regional Infrastructure Security and Disaster Resilience

PNWER has been working since the September 1, 2001 attacks to develop ways and avenues for information sharing among the public and private sectors and other stakeholders through outreach, developing and conducting workshops, exercises, interdependency forums, pilot projects and leading/facilitating Partnership activities, including regular meetings.

PNWER is unique in that it has a statutory mandate from five states: Alaska, Washington, Idaho, Oregon, and Montana, as well as the western Canadian provinces of British Columbia, Alberta, and the Yukon. PNWER’s board is made up of elected state and provincial legislators, the Governors and Premiers of all jurisdictions, and Industry leaders in the major industries in the bi-national region. Our focus is the economy of the region, and the safety and quality of life for all citizens. After September 11, our governing board was very concerned about the safety of our communities, as well as safeguarding against the potential threats to our economy. In consultation with all Governors and Premiers, it was agreed that the one area that was not being fully addressed was the interface between private infrastructures and government. It was this gap that PNWER’s Center for Disaster Resilience was launched to address.

Throughout the winter of 2002, the Pacific Northwest Partnership for Regional Infrastructure Security created by PNWER began preparation for the first multi-sector, multi-jurisdiction, cross border exercise focused on critical infrastructure interdependencies called Blue Cascades. This unprecedented exercise was the first in a series and was held outside of Portland, OR in June 2002 and was attended by more than 200 representatives from all eight jurisdictions in the PNWER region. The exercise was based on a terrorist attack on some of the Bonneville Power Administration’s important assets, bringing down much of the northwest power grid for weeks to months. The exercise focused on cascading impacts involving all critical infrastructure sectors, as well as law enforcement. It was eye-opening to all participants

After Blue Cascades I, We continued to have quarterly meetings of the Partnership, and held an Action Planning meeting to address shortfalls identified in the exercise. This process led to a regional Action Plan comprised of a number of recommended initiatives, some of which have been accomplished and some which are ongoing. The most notable finding from the exercise

was the high priority all stakeholders placed on the need for a regional information sharing mechanism for all key stakeholders. We took this identified need to the then Whitehouse Office of Homeland Security – CIO Steve Cooper, and Col. Bob Stephan. In the spring of 2003 we hosted a meeting with the Seattle FBI to establish a pilot for the northwest which became the NorthWest Warning, Alert, and Response Network (NW WARN.GOV).

NW WARN developed a public – private board of key stakeholders, and a gatekeeper community of over 100 key leaders in all 17 infrastructures. We petitioned to become a pilot project in a new program DHS was launching based on the Dallas, TX Emergency Response Network (ERN), which was a largely law enforcement-focused model out of the Dallas FBI. After much delay, DHS agreed to let us be part of the new pilot, which became known as HSIN-Critical Infrastructure or HSIN-CI.

Over the past four years, we have worked to build the membership of this information sharing system to over 2,000 vetted key stakeholders in our region. We developed a handbook, detailed requirements for information sharing among sectors, but never received the support we needed from DHS for implementation. Instead, Last month, DHS discontinued the program and sent a letter to all 2000 professionals to announce the cancellation. Our NW WARN Board nonetheless has continued to meet, and we are determined to build the functionality into the system that we have always wanted to be able to share critical information among sectors and with law enforcement and emergency management.

Blue Cascades II – focus on Cyber Systems

Key stakeholders elected to develop a second regional interdependencies exercise with PNWER’s help the following year. Blue Cascades II was again a grassroots effort to address an issue that the first exercise had left out – cyber vulnerabilities and the gap between physical and cyber preparedness. A Scenario Design Team, made up of over 30 organizations, labored over six months developing the scenario, which brought out the importance of cyber systems and information security..

The process of bringing private sector key individuals, who live and breathe the vulnerabilities of their systems, together with law enforcement and emergency management was incredible. We had every participant sign a non-disclosure agreement to participate in the exercise. For many first responders, it was the first time they realized just how the communications systems they relied upon could be compromised by a cyber attack that could leave them essentially ‘in the dark’ and unable to communicate.

The exercise led our state Homeland Security Director to state that were it not for the exercise, he would not have known about what he considered one of the top five vulnerabilities in the state – pointing out that both DOD and DHS had missed listing this particular issue on their state-wide assessment, but was brought out by the process of stakeholder information sharing during the exercise.

Blue Cascades III – focus on Earthquake Preparedness

Following Katrina, stakeholders met to discuss what was the Northwest’s ‘Katrina’. All agreed that it was the 9 point subduction zone earthquake that is anticipated to hit off the coast from British Columbia to California sometime in the next 50 years or so. (The last one was on Jan. 26, 1700, and records show that it has happened on average every 300

years). This exercise was led again by PNWER with critical infrastructure stakeholders who wanted to address the long term recovery and reconstitution issues after an extreme disaster. It was a two day exercise involving over 350 participants.

Lessons Learned for Information Sharing. While previous Blue Cascades exercises demonstrated the need for interoperable communications, in BLUE CASCADES III at issue was the impact of the loss of telecommunications and critical IT systems and how these systems and particular emergency communications could be made more resilient (able to withstand a subduction zone quake and expeditiously recover with minimal damage). Some participants pointed to mitigation measures, including building more systems redundancy and developing alternative, mobile, and easily deployable wireless-based communications. There was need for “situational awareness”—knowledge of what was happening throughout the region—as the disaster unfolded, to enable optimal decision-making on response (e.g., dispatching personnel and other resources where needed, prioritizing service restoration, determining evacuations routes and sheltering locations, etc.). Private sector and other non-government organizations emphasized the need for their inclusion in regional preparedness planning, not just with the state or provinces, but with municipalities. One water systems representative stated that he would like to hear from government less of “I got you covered—don’t worry” and have more cooperation. An energy official noted that “cooperation is a two-way street and public and private sector representatives must be willing to meet and participate in the many infrastructure and planning initiatives currently underway, and not just at the exercises that come along every now and again.” A telecommunications representative reflected sentiments of other participants that companies are reluctant to share information directly with government. Through participating in “lots of exercises”, however, they can determine what information they need and what needs to be shared. As one participant put it, “Trust relationships are paramount in creating an environment where it is felt that information can be shared safely, and in confidence.” A power company official cited the need to know what the critical loads are for the other sectors and that without this knowledge it would be difficult to establish restoration priorities. Non-electric sectors wanted to learn more about how power is capable of being restored and work with utilities to make modifications to their systems so restoration of power to critical infrastructure can be accomplished quicker.

The Blue Cascades III scenario of an earthquake—an unexpected act of nature—precluded the need for participants to address alert and warning in the Puget Sound Region through NWWARN. A major issue, however, was the tsunami warning system. Participants questioned whether the many thousands of individuals along the coast from British Columbia to San Francisco would have ample warning time to reach higher ground, or even receive a warning given the widespread regional power outage and telecommunications failures generated by the earthquake. On response or recovery/restoration issues, it was unclear in the exercise how decisions would be made on trade-offs that needed to be made within a short time frame. An example was the issue of whether to use scarce water for putting out the fires from gas leaks and pipe ruptures or to save it for human consumption. Moreover, organizations had no way to gain information on what resources were available. For example, Cingular noted that it has “loaner” cell phones, portable cell phone sites, and cellular phones that plug into laptop computers to create internet connectivity. The federal government was said to be working on a process to channel private sector assistance to government authorities in a crisis,

There was much discussion in Blue Cascades III on priorities regarding service restoration in an environment when there would be great demand and competition for being towards the top of the

prioritization list. Some participants pointed out that states, localities, and utilities had already established priority lists, and these should be followed. Other participants, such as the Postal Service, expressed concern that they were far down on the list and would not gain services for “some period of time”. Still others noted that priority restoration should be flexible depending on need. At the same time, most participants appeared to understand that in a major disaster priority lists would likely “go out the window”, and that infrastructure interdependencies should play a role in which services were restored and in what sequence. As one participant put it, “priorities are different depending upon where you sit.” In addition, there was also some discussion related to what is most critical. Participants questioned whether it is the water supply system, hospital, transportation, food and agriculture operation, or life safety such as emergency services. As an electric power representative observed, “understanding what ‘critical load’ is will help establish restoration priorities.”

Blue Cascades IV – Pandemic Preparedness and Critical Infrastructures

Blue Cascade IV held in January of this year focused on impacts on critical infrastructures and essential service providers from a Pandemic Influenza attack. We included the excellent experience of the Ontario Emergency Management director who had handled the SARS epidemic in Canada, and looked again at the interdependencies of our critical infrastructures and how there might be cascading impacts due to workforce shortages. It was evident that more needs to be communicated to private sector critical infrastructures, and that HHS and DHS need to be better coordinated for incident management in a Pandemic.

We were fortunate to have the HHS Director of Critical Infrastructure Protection, Dr. Tom Sizemore for a planning session for the exercise and have the Regional Director for HHS participate in the event..

Again, it was clear that information sharing among critical infrastructures, government, and public health agencies was absolutely vital, and not being well addressed. Our region has some of the leading private sector businesses who have done landmark work in Pandemic preparedness and were willing to share their efforts with their peers. Boeing, Microsoft, Washington Mutual, Puget Sound Energy, Starbucks, Bonneville Power Administration are some of the leading companies in this area in the world. We are in the process of developing an Action Plan based on the lessons learned from the most recent exercises that can become part of a regional pandemic preparedness strategy.

Recommendations:

The following are based on PNWER’s long experience of working with stakeholders to develop and implement regional disaster preparedness initiatives.

The Federal Government should fund the start up and provide technical support to develop regional public/private partnerships in communities and states addressing regional resiliency, public/private information sharing, and critical infrastructure security. This could be done by a competitive program providing up to \$250K to allow seed money for interested states and regions to move forward and develop an ongoing process to build trust and develop awareness among key stakeholders of public and private infrastructures on vulnerabilities and mitigation measures associated with regional interdependencies.

The eight jurisdiction PNWER region is demonstrably ahead of the nation in building cross-sector trust among regional stakeholders to foster disaster resilience. DHS, the Department of Defense, and other federal agencies can use the PNWER region as a test-bed to work with regional stakeholders to develop solutions for the critical challenges that face the nation today – including developing a model regional public/private sector, all-hazards information fusion center and the protocols and procedures to allow virtual information sharing among all critical infrastructures, law enforcement, emergency management, and other key stakeholders. PNWER commends certain federal agencies, DHS/ Science and Technology Directorate, the Defense Threat Reduction Agency, and the U.S. Department of Energy for willingness to provide modest support for a few significant projects focusing on interdependencies challenges. Much more of this type of support needs to be provided to undertake many of the recommended solutions to preparedness shortfalls identified in the respective Blue Cascades exercises that are enumerated into the Blue Cascades Integrated Action Plan.

Summary

To summarize, in addressing disaster resilience, our focus must be not just inside organizations or on sectors but outside the fence, cross-sector, grass roots to national level, focus on all threats (including aging and deteriorating infrastructures), and all-hazards and regional in scope. We must reminder always that all disasters are local and that all trust is local.

We have to also keep in mind the “Resilience Tautology”—that resilient assets and infrastructures require resilient regions; regional resilience requires an understanding of infrastructure interdependencies and associated vulnerabilities, consequences of disruptions under specific scenarios, and risk-based mitigation; and that regional risk assessment and management requires collaboration and information-sharing among key stakeholders, which includes regional DOD assets.

Lastly, federal support—funds and technical assistance and encouragement—is essential to spearhead, develop, and initially sustain cross-sector collaboration to identify needs and cost-effective solutions—activities and pilot projects—to meet homeland security and disaster resilience challenges. In the area of information sharing, it is important to move forward with support for developing a regional information fusion center that incorporates the private sector that can be a model for the nation. Following is a description of this essential pilot project for which PNWER has been tasked to set up and facilitate a Task Force to develop.

REGIONAL INFORMATION FUSION CENTER PILOT PROJECT

Purpose

The following testimony outlines what is required to build on existing capabilities for cross-jurisdiction/public-private collaboration and information-sharing to develop a **state-wide, holistic regional information sharing and analysis capability** to meet the following broad security and disaster resilience needs:

1. Collection, integration, analysis, and dissemination of all-source threat-related information for law enforcement and infrastructure protection;
2. Understanding regional interdependencies and determining critical infrastructure/key resources (CI/KR) vulnerabilities and risk;
3. Disaster/incident preparedness and management.

The pilot project would encompass and leverage various activities supported by components of the U.S. Department of Homeland Security that currently are underway to improve regional information sharing and analysis capabilities, including the Washington Joint Analytic Center (WAJAC)) and the developing Seattle/King County fusion center; NWWARN, and the Puget Sound Partnership Interdependencies template project. The pilot project would also leverage systems and procedures for information sharing already developed by DHS, DOD and other entities.

The end-result would be a state-wide “virtual” Regional Information Fusion Center (information sharing and analysis capability) with protocols/procedures that can cost-effectively provide public, private and other key stakeholders with appropriate, secure, resilient, two-way interaction at the local, state, and federal (civilian and defense) level. This capability would connect and enhance but not replace mission-specific state and local emergency management, law enforcement, defense, and other systems and mechanisms, including EOCs, Special Operations Centers, Law Enforcement Intelligence Operations, Dispatch Centers, etc.

This pilot project would provide a model which could be customized by states and localities across the nation.

Background

Since the September 11 attacks more than five years ago, acquiring information on threats to infrastructures, vulnerabilities, and impacts has been a top priority and essential for determining CI/KR criticality and risk. At the national level, sector-focused Information Sharing and Analysis Centers (ISACs) were established. As understanding grew of infrastructure interdependencies and the need for identifying asset criticality and managing disasters, regional public-private partnerships emerged in some parts of the country. A major objective of these partnerships was to facilitate regional information sharing by building trust among key stakeholders and cooperatively identifying security and preparedness gaps.

At the same time, in states and municipalities nationwide, law enforcement authorities created information and intelligence sharing and analysis mechanisms to focus on threats and crimes. Today there are more than three dozen of these information fusion centers in various stages of development and reflecting the cultural and jurisdictional interests of the areas they serve. Their goal is to develop the technologies, procedures, analytic staff and capabilities to integrate and assess relevant law enforcement and intelligence information, coordinate security measures, and facilitate two-way flow of timely, accurate, actionable information on all types of hazards. The focus, scope, functions, participation, and organizational structure of these centers are evolving as understanding of the requirements increases. A series last year of four Information Fusion Center Regional Conferences sponsored by Department of Justice with the U.S. DHS for

managers of state and local Centers identified many issues that remain to be resolved. Some of the more important of these issues are:

- Expanding the focus of the Centers to cover all threats, all crimes, and all hazards;
- Inclusion of critical infrastructures and essential service providers and other key stakeholders with focus on two-way information-sharing;
- Creating and maintaining regional situational awareness pre and post incident; and
- Outreach to communities, including associations serving ethnic and special needs groups.

A priority issue is developing a *virtual capability* (i.e., procedures, technologies, organizational structure, and supporting concept-of-operations) to link information fusion centers and other collaborative mechanisms and key stakeholder organizations in a state-wide or broader regional interoperable network to accommodate diverse multi-jurisdiction needs, geographic realities and cultural and infrastructure sector interests. This virtual Regional Information Fusion Center would have two-way information sharing based on a multi-layered secure and resilient system with analysis produced by a team of core resident local and state experts and virtual analysts from different sectors and disciplines using a largely virtual database to enable integration, assessment, and secure, tailored dissemination of information provided to key stakeholders. This analysis would be used for organizational and collective decision-making and crafting public information.

This virtual capability will interconnect state, local, private sector and other stakeholder capabilities while avoiding of duplication of effort, proliferation of analytical products, and competition for scarce analytical staff resources. It will also enable federal authorities to have a single focal point for effectively and securely providing intelligence and other sensitive information to a wide range of “customers”.

Activities within Washington State that Can Be Leveraged

Washington State is well ahead of many other regions in the nation with an established information fusion center operated by the State Patrol and situated in the FBI Building in Seattle. The WAJAC is in the beginning stages of bringing in private sector analysts. At the local level, King County with surrounding counties have been developing regional preparedness plans and working with key stakeholders to address vulnerabilities and impacts associated with infrastructure interdependencies.

A public-private Partnership for Regional Infrastructure Security has been in existence since 2002. There have been four regional interdependencies exercises developed and conducted by the Partnership thus far, each focusing on a different type of threat scenario—physical and cyber attacks/disruptions, natural disasters (subduction zone earthquake) and an influenza pandemic. These exercises have resulted in recommendations for creation of a Regional Information Sharing and Analysis Center (regional ISAC) to enable key stakeholders to prepare for and manage disasters from terrorist attacks, natural disasters or other causes. In addition, Partnership members are currently testing an automated interdependency template developed for them by DHS/S&T/CIP and have created an Information Sharing Working Group to develop secure

information sharing procedures for private sector organizations to exchange agreed interdependencies data collected internally with the template.

There is a community-focused alert and warning system, NWWARN, and the City of Seattle and King County are looking towards developing an information fusion capability to serve local law enforcement needs that would include critical infrastructures and essential service providers. Various proposals and some work are underway on enhancing these existing capabilities. The City of Seattle Police Department and the Pacific Northwest Laboratory have been collaborating on technology and procedural requirements for a Seattle/King County regional fusion center. ESRI is developing a virtual analysis system for use by fusion centers. There are plans to enhance WAJAC's collection, analysis, and dissemination of information and intelligence to law enforcement and non-law enforcement agencies through developing effective Regional Intelligence Groups (RIGS) and creating a Threat Early Warning Group (TEW) system.

Pilot Project Overall Goal

The goal of the proposed pilot project is to develop a statewide virtual regional cross-sector, cross-jurisdiction, secure, and resilient two-way information sharing capability that:

- Protects proprietary data;
- Utilizes existing procedures and mechanisms;
- Focuses on all threats, all crimes, and all-hazards;
- Identifies vulnerabilities, security and preparedness gaps, and assesses risk;
- Meets local law enforcement needs;
- Has a state-wide scope and reaches outside state boundaries and cross-border to address regional interdependencies;
- Supports the alert and warning function of NWWARN and incorporates member organizations as appropriate;
- Supports Emergency Operations Center Disaster Management Activities;
- Undertakes outreach and educates community groups;
- Fosters interoperability and standardization;
- Provides federal agencies through a single focal point access to state, local, and regional key stakeholders.

Note: Specific Task list for the Fusion Pilot is listed in the Attachments