National Infrastructure Protection Center

August 7, 2002

Blue Cascades Table Top Exercise
Pacific North-West Economic Region

NIPC participated in the Blue Cascades exercise sponsored by Pacific North West Economic Region (PNWER). The exercise revealed the complexities of major critical infrastructure outages and their impact on the PNWER. The Blue Cascades Final Report Executive Summary (can be found online at http://pnwer.org/pris/CascadesReport.htm) is attached as an example of how to bring an economic region together for the purpose of identifying its vulnerabilities and formulating plans to deal with them.

The Blue Cascades tabletop exercise is an excellent example of an effort to implement the "National Strategy for Homeland Security."[1] It is indicative of the greater value that can be achieved on a local/regional level as well as national in infrastructure protection.

States are encouraged to contact PNWER or the NIPC for information on how to bring together regional leadership for infrastructure protection efforts.

PNWER is a statutory private/public partnership designed to facilitate cooperation, coordination, and communication among its members. PNWER includes Oregon, Washington, Idaho, Montana, and Alaska in the United States and Yukon, British Columbia, and Alberta provinces in Canada. PNWER's goals are as follows[2]:

- To increase the economic well-being and quality of life for all citizens of the region.
- To coordinate provincial and state policies throughout the region; to identify and promote "models of success;" and to serve as a conduit to exchange information.

Following the attacks of September 11, PNWER determined that a better understanding of the interdependencies among critical infrastructures was needed in the region. Over the past nine months, it planned and implemented a tabletop exercise, called Blue Cascades, to identify those inter-dependencies.

PNWER can be contacted at (206) 443-7723/7724, or matt@pnwer.org.

NIPC can be contacted at (202) 323-3205, or nipc.watch@fbi.gov.

[1] The "National Strategy for Homeland Security" establishes that "protecting critical infrastructure and key assets" is one of six critical mission areas[1]. A key element in achieving this mission is establishing and maintaining "effective partnerships with state and local governments and the private sector". Since its inception, the National Infrastructure Protection Center (NIPC) has been performing this mission through Information Sharing and Analysis Centers (ISACs), the Infragard program, and direct support to critical infrastructure sectors. (National Strategy for Homeland Security, Office of Homeland Security, *July 2002* http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

[2] Please see the PNWER website at http://www.pnwer.org

Pacific NorthWest
Economic Region

Infrastructure Interdependencies Tabletop Exercise

"BLUE CASCADES"

Held June 12, 2002
in Welches, OR

Final Report

Executive Summary

July 18, 2002

BLUE CASCADES
Infrastructure Interdependencies Exercise
Final Report

Executive Summary

More than 150 representatives from 70 private and public sector organizations attended the first of its kind multi-jurisdiction, cross-border tabletop infrastructure interdependencies exercise on June 12, 2002 in Welches, Oregon. The exercise was conducted by the Pacific NorthWest Economic Region (PNWER) and co-sponsored by the U.S. Navy, Federal Emergency Management Agency (FEMA Region 10), and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

BLUE CASCADES was the second in a series of activities that are elements of a unique initiative— the Partnership for Regional Infrastructure Security— launched by PNWER in late 2001 with the goal of developing a cooperative preparedness strategy using a risk-based approach to enhance the security of critical systems region-wide.

PNWER, chartered in 1991, brings together public and private sector interests with the aim of enhancing the economic development of its eight U.S. and Canadian member jurisdictions: Alaska, Alberta, British Columbia, Idaho, Oregon, Montana, Washington, and the Yukon Territory. The first activity was the Partnership kick-off meeting on Nov. 30, 2001 in Spokane, Washington, attended by over 120 private and pubic sector organizations from all the jurisdictions that comprise PNWER.

The exercise focused on the linkages between and among infrastructures that could make the Pacific Northwest vulnerable to cascading impacts in the event of an attack or disruption, and which could complicate expeditious response and recovery. Critical infrastructures participating in the exercise included energy (electric power, oil, and natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. Federal, state/provincial, and local government agencies, including emergency management organizations, were also well-represented.

BLUE CASCADES was expressly designed to help stakeholders assess the current state of their understanding and preparedness, particularly from the perspective of infrastructure interdependencies. It also was aimed at identifying their needs, priorities, and resource requirements for incorporation into an Action Plan to assist the eight jurisdictions within PNWER to become a disaster-resistant/resilient region.

During the exercise, players addressed a challenging scenario that was developed by a group of stakeholders representing private and public sectors from PNWER's jurisdictions. Organizations contributing to the scenario included Bonneville Power Administration, BC Gas, BC Hydro, Boeing, Duke Energy, PG&E, Williams Gas Pipeline, Puget Sound Energy, Port of Seattle,Idaho Bureau of Disaster Services, U.S. Navy, the National Infrastructure Protection Center, Telus, Verizon, Qwest, FEMA, BC Provincial Emergency Program, and OCIPEP.

The scenario reflected those threats that the exercise participants were most concerned about — both deliberate and "non-deliberate," with particular emphasis on the type of high-profile terrorist threat that is dominating today's headlines and which could cause cascading, long-term impacts. The terrorist attacks, physical in nature and directed at disrupting the region's electric power, caused region-wide power outages that quickly spread to other western states. There were follow-on disruptions of the region's telecommunications and natural gas distribution, as well as a threat to a major municipal water system and to the region's ports. The attacks and disruptions of critical services and related response and recovery actions impacted other interdependent infrastructures, including transportation, emergency services—hospitals, mass care—and law enforcement. Cross-border issues and challenges were highlighted. Relevant operational information provided by a Scenario Design Group made the scenario as realistic as possible.

The scenario provided an impetus for participants to discuss infrastructure interdependencies and infrastructure protection, mitigation, response, and recovery requirements across government agencies and the private sector. Participants grappled with a series of questions that enabled them to explore how a complete disruption or a service curtailment in one infrastructure could cause cascading effects on other infrastructures, and how infrastructure interdependencies could exacerbate repair and restoration efforts. Evaluators from participating organizations, as well as independent evaluators, provided immediate feedback to participants.

These evaluators subsequently submitted detailed comments on the strengths and shortfalls arising from BLUE CASCADES. These observations and feedback from evaluation forms completed bythe participants formed the basis of the exercise final report and will be reflected in an Action Plan to be addressed by stakeholders when Partnership member organizations reconvene in September.

Overall, participants found that BLUE CASCADES had met its objectives and were grateful for PNWER's leadership and facilitation role in identifying the challenges raised by infrastructure interdependencies. They found the exercise was particularly

effective in illuminating what they know and don't know about regional interdependencies, and the preparedness gaps they need to address to create a disaster resistant/resilient region. Participants expressed the need for further such multi-jurisdiction, cross-national activities.

Seventy-five percent of responders rated BLUE CASCADES a four or five out of a possible five points on an evaluation form; comments included:

"BLUE CASCADES was a good opportunity to exercise 'as a team' in preparation for the real thing. The fact that different agencies networked with each other was a big step forward. This was an extremely valuable way to get discussions going on the priorities of individual sectors, especially when those priorities may be in conflict."

"It brought out a number of questions (about) emergency preparedness that I had not thought about." "It gave me a better idea (of) how vulnerable our critical infrastructure really is."

BLUE CASCADES "helped open my eyes to interdependencies."

"The scenario was plausible and timely; the resulting discussion provided me with action items to take to my organization."

"Just the fact that the different agencies networked with each other was a big step forward."

"*There was constructive disagreement and debate. This was the best discussion I have heard on the complex interrelationships of critical infrastructures in the Pacific Northwest region."*

Key Findings

Infrastructure Interdependencies

- Organizations represented demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities, and operational dynamics of these regional interconnections, particularly during longer-term disruptions.

- Many participants initially assumed their organization's contingency plans for addressing natural disasters or isolated emergencies would be adequate in responding to significant terrorist attacks and disruptions and multiple events. However, they came to realize that interdependencies could void or negate those assumptions.

- There was little recognition of the overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans, and the need for contingency plans in the event of loss or damage to electronic systems.

Cooperation and Coordination

- There was minimal coordination of activities and little or no understanding of other organizations' interests, response plans, or restoration priorities.

- There was no region-wide strategy to strengthen security, enhance preparedness, or coordinate emergency response within and across sector and jurisdictional boundaries.

- Law enforcement and industry/private sector cooperation and coordination were limited, with no forum to bring together key law enforcement and security personnel to share information and discuss matters of mutual concern.

- U.S. and Canadian cooperation was seen as limited in the areas of law enforcement, response and recovery and information sharing; at the same time, there was a lack of understanding of what cooperation does exist.

- The range of services that federal civilian and defense agencies could provide during regional emergencies was not clear. Also, information was lacking on how regional national defense facilities, with significant dependencies on commercial infrastructures, would coordinate with these infrastructures.

Communications

- Participants had difficulty envisioning a situation in which they would lose telephonic and internet communication and lacked contingency plans to work around the problem.

- Although many organizations had radio back-up, it was unclear how often these systems were tested. Based on exercise discussions, there would be little if any interoperability with other stakeholder communications systems.

- Law enforcement lacked an effective way to disseminate and receive threat-related information from private sector organizations and utilities.

- There are no established protocols or regional networks to facilitate rapid and reliable dissemination of outage-related information to critical community organizations and infrastructures.

Resources

- All sectors faced resource constraints to various degrees, including critical components and equipment, and skilled personnel for recovery activities.

- Participants did not take into account the demand on the part of other organizations and businesses to secure scarce additional back-up power generation, including fuel for generators. They also did not appreciate the need to prioritize those demands.

Reporting and Analysis

- There is no common, continent-wide alert system with threat levels that have a corresponding set of actions required.

- The new color-coded alert system established by the U.S. Office of Homeland Security appeared to be little understood, and conflicted with infrastructure sector threat levels.

- There is no mechanism for cross-border sharing of U.S. and Canadian threat-level information or a common color-coded terrorist alert system.

- There are few, if any, regional or industry-sector clearinghouses for threat or incident-related information that can be used for planning and response.

- There are no dedicated communication channels for infrastructure stakeholders to use to report information to federal, state/provincial, and local government agencies to prevent being swamped by requests for status reports.

- Modeling and simulation capabilities do not yet exist that can help assess economic and other damage from prolonged regional disruptions.

Command and Control

- Roles and missions of the various government authorities at all levels in a large-scale regional terrorist attack or disruption were unclear.

- Participants expressed concern over whether law enforcement should take precedence over restoration, citing designation of critical assets as crime scenes and failure to take into account economic impacts of counterterrorism actions.

- There is a general lack of guidelines on preservation of evidence within private sector organizations.

- Lines of authority were unclear among the FBI and other U.S. and Canadian federal, state/provincial, and local law enforcement entities, including the role of national defense. This was seen as particularly problematical regarding port security.

Public Information

- Coordination and dissemination of public information emerged as one of the greatest challenges in a regional infrastructure disaster that involved terrorism.

- Little attention was paid to the all-important "human factor"—that people will panic and believe rumors in the absence of accurate, instructive information.

Selected Recommendations

- ***Improve Understanding of Regional Interdependencies*** by undertaking region-wide identification of what assets are most critical, conducting physical and cyber vulnerability assessments, and identifying/assessing interdependencies.

- ***Develop a regional threat assessment approach*** that takes into account international and domestic adversaries, critical regional assets, and vulnerabilities; leverage work done for Y2K by jurisdictions and the private sector.

- ***State/provincial and local governments should review,*** with private sector input, ***emergency response plans and mutual aid agreements*** to assure that terrorism and interdependencies-related challenges are addressed.

- ***Develop training modules; hold targeted workshops and exercises*** to further address interdependencies issues raised in BLUE CASCADES (e.g., port security; protection of the industrial base).

- ***Develop a secure, regional clearinghouse for interdependencies issues and related preparedness information***, including data on all regional exercises and training opportunities.

- ***Undertake the development of analytic tools to provide credible damage assessments*** for use in preparedness planning and to assist in response and recovery.

- ***Develop a regional nuclear/radiological preparedness program*** that takes into account private and public sector security and response/remediation needs.

- ***Utilize the Partnership for Regional Infrastructure Security to develop a common terminology and preparedness plan for the region***, facilitate exchange of information and monitor the progress of implementation.

- ***Consider the need for a Utilities Regional Security Association (URSA) under the auspices of the Pacific Northwest Economic Region*** modeled along the lines of the California Utilities Emergency Association. URSA would provide a list of regional points-of-contact in all state/provincial, local, law enforcement organizations and utilities, as well as a forum for planning and coordination.

- ***Establish a Maritime Security Coalition as part of a Port Security initiative*** to bring key stakeholders together and address unique port security needs

- ***Foster development of joint U.S.-Canadian protocols, MOUs and collaborative activities*** to address significant law enforcement and consequence management issues, including research and development of analytic tools and technologies to assess regional impacts and mitigate vulnerabilities.

- ***Identify the range of federal civilian and defense resources*** that can be brought to bear to address regional response and recovery needs.

- ***Seek legislative support for necessary policies and technical assistance programs*** to meet regional protection, mitigation, response and recovery needs, including training, exercises; also, information sharing (e.g., relief from freedom of information act and sunshine law requirements).

- ***Explore options for, and establish, a secure, region-wide common communications network*** with sufficient redundancy and alternative systems.

- ***Develop procedures to facilitate the dissemination of outage-related information*** expeditiously to key infrastructures.

- ***Establish stockpiles and procedures for prioritized access to electric power generators, other emergency back-up equipment, and also critical components*** that would be difficult to obtain in the short-term.

- ***Work with appropriate government organizations to put in place a common, public-private sector, continent- wide, alert system*** with threat levels that have standardized actions required.

- ***Set up a region-wide, cross-border threat information exchange mechanism*** and threat data repository.

- ***Delineate roles and missions of government authorities*** in regional terrorist-initiated disruptions.

- ***Develop guidelines for law enforcement and private sector organizations outlining crisis and consequence management*** procedures and priorities.

- ***Develop guidelines for effective and expeditious dissemination to the public of information about outages***, including duration, resulting safety factors, and providing instructions on what they should and should not do. Development of such procedures should take the "human factor" into account.

- ***Establish a mechanism to coordinate public information during regional emergencies***.