BLUE CASCADES II
Action Plan

Participants of the BLUE CASCADES II Interdependencies Tabletop Exercise reconvened on November 12 in Redmond, Washington to develop an initial, flexible Action Plan of projects to meet regional preparedness needs identified during the exercise. BLUE CASCADES II focused on a multi-faceted scenario that involved physical and cyber attacks and disruptions and associated infrastructure interdependencies. A particular emphasis was on prolonged outages of critical services that had significant impacts on the economy and public welfare.

BLUE CASCADES II was designed to raise awareness of regional preparedness shortfalls and point to cost-effective solutions. The exercise produced a large number of findings on shortfalls and developed recommendations to address these issues that were then incorporated into a Final Report. These gaps were in the following six general areas: (1) understanding interdependencies, cyber threats and disruptions; (2) cooperation and coordination; (3) communications and information sharing; (4) roles and responsibilities (incident management); (5) resource management; and (6) public information and education. (See Appendix.)

Action Planning Process. To help generate ideas and prioritize useful projects, Working Groups were created for the Redmond meeting in order to focus on the six broad areas of preparedness needs identified in the exercise. Two successive sessions comprised of three of these Working Groups met simultaneously, enabling each participant to contribute to two of their choice —one Working Group per session. Each Working Group was facilitated by two co-moderators—one from a public organization and the other from the private sector. Working Group participants were provided with "issues papers" that described the problem set for each of the six areas, including questions to generate discussion and help identify useful activities. Working Groups were instructed to identify short-term (i.e., "low-hanging fruit"), medium term and longer-term projects that stakeholders could collectively and individually undertake to address shortfalls highlighted in the exercise. All participants then met in a final plenary session to hear each of the Working Groups report on their recommendations for projects. The candidate activities from the Working Groups were discussed after the meeting by members of the exercise Scenario Design Team and then combined with further ideas from participants'

written evaluations of the meeting, as well as additional concepts submitted by other stakeholders. This integrated list became the basis of the Action Plan.

Results of Action Plan Meeting Discussions

The half-day meeting marked only the start in identifying specific projects in what will be an ongoing task to improve regional preparedness. The short time for the Working Group sessions did not allow for more than a cursory discussion on many of the projects. Also, the number of exercise recommendations was extensive, with many that went across two or more of the six categories of needs. An additional constraint was the different organizational backgrounds of participants, prompting one to observe that "…we must start speaking in simple language, without all the bureaucratic jargon." Lastly, many of the participants are only just beginning to tackle the complexities of infrastructure interdependencies, regional preparedness requirements and cyber security challenges. U.S.–Canadian cross-border interdependencies and cyber issues, for example, are only just beginning to be addressed.

That said, the meeting produced a large number of candidate projects. A few of them were sweeping in scope and more appropriate to be undertaken at the federal level. Most, however, were "doable" activities at the local and state levels.

Working Group Deliberations

Understanding Interdependencies, Cyber Threats and Disruptions (BLUE CASCADES II Recommendations 1-5)

This discussion centered on what actions could be undertaken to gain greater understanding of interdependencies and related physical and cyber vulnerabilities, impacts and operational dynamics, including possible mitigation measures. Issues addressed included the need to develop criteria on when to stand up an Emergency Operation Center (EOC) for a cyber attack; and how to educate stakeholders, media and legislators on these issues, including power outages and rolling blackouts. There also was discussion on how a "classification" scheme could be developed to facilitate information sharing but protect the information from public release; developing a "roadmap for new cyber threats; and undertaking pilot projects with U.S. CERT, the Department of Homeland Security, Federal Bureau of Investigation and other federal agencies. Regarding interdependencies, suggestions included development of toolsets and templates to identify and assess these cyber and physical interdependencies at deeper levels. Also development of a secure database to house the information was identified along with a project to map regional cyber-physical interdependencies and a regional cyber education and awareness program. Among the more far-reaching projects raised were creation of a backup, secondary Internet--such as the Defense Department is currently undertaking.

Cooperation and Coordination (BLUE CASCADES II Recommendations 6-17)

Discussions focused on how to achieve the level of coordination and cooperation necessary to improve regional preparedness and expedite response and recovery from disasters, including cyber attacks and disruptions. Issues addressed included how stakeholders could share information on

response and recovery plans/practices and build upon existing mechanisms to develop regional plans and other means to improve readiness. Ideas raised included creating a regional Cyber Security Council that could address policy, legal and public disclosure issues related to cyber information sharing and analysis; also, developing protocols for information sharing and a mechanism to expedite clearances for appropriate private sector staff. Other activities included development of a "yellow pages"—a resource directory of points-of-contact, including "who does what"; a cyber security self-assessment handbook for government and private sector organizations, and a cyber "First Aid Handbook" to provide information to organizations on incident response and recovery.

Communications and Information Sharing (BLUE CASCADES II Recommendations 18-22)

Discussion centered on how to deal with legal and proprietary barriers to sharing information among public and private organizations and other challenges related to communications and information exchange. Projects suggested included development of public disclosure exemptions, developing and conducting a workshop on the National Incident Management System (NIMS), improving the NW WARN information exchange system to evolve it into a Regional Information Sharing and Analysis Center (ISAC) for threat analysis and other information. Also suggested was the creation of a centralized calendar of exercises and other homeland security and emergency preparedness events, and an inventory of what backup communications systems and resources are available when phones and Internet are disrupted.

Roles and Responsibilities (BLUE CASCADES II Recommendations 23-25)

Discussions addressed the challenges facing regional stakeholders in sorting out the roles and responsibilities in incident management, with emphasis on cyber events -- an area where much work remains to be done. The issue of who is in charge was addressed. There was considerable focus on NIMS, what it is, federal expectations about NIMS compliance (which remains unclear), and how NIMS will be implemented and funded. There also was discussion about how to get the private sector involved in NIMS and what outreach program might be required to raise awareness in this regard. The value of drills and exercises was underscored, particularly as the best way to understand interdependencies. The recent Florida hurricanes and the Mt. St. Helens eruption were raised as events that helped better refine emergency plans in the region. Also addressed was effectiveness of incident management in the past and the need to look at previous events to assess this concern. Another proposed activity was the need for a regional reporting system for cyber attacks. Other ideas for activities included investigating how the private sector could become integrated in NIMS, development of a Regional Incident Response Plan, creation of a regional reporting system for cyber attacks, and a very key issue--identification of a central and single-point-of-contact within the federal government for cyber security and incident response.

Resource Management (BLUE CASCADES Recommendations 26-29)

Working Group participants looked at the problem of lack of management strategies for large-scale disasters, including cyber incidents and how necessary personnel, equipment and other resources could be accessed and secured. Suggestions for projects included development of a

resource inventory process that would entail assessing available options and recommend a process to support emerging state and NIMS standards for definitions, data collection and sharing. This process could be expanded to private industry and ultimately include cross-border assets and resources. Another proposed activity was to assess the resources and capabilities of research organizations to provide information and training on threats and vulnerabilities (including SCADA system vulnerabilities), weapons of mass destruction, and what resources would be needed to deal with various types of natural and man-made disasters. Also proposed was development of a process to educate private sector organizations about response levels and developing a process for allocating resources and/or reimbursements for response and recovery. Other projects suggested were development of a way to improve understanding of common definitions that would be part of a broader education process for public and private stakeholders, a method to benchmark best practices of other regional initiatives, and a process to facilitate the efficient movement and travel of first responders and other critical personnel across state and national borders in an emergency.

.

Public Information and Education (BLUE CASCADES II Recommendations 30-33)

Discussion focused on the lack of a public information and education strategy that would enable the general public and the media to receive necessary, accurate, and coordinated information during a major regional disaster, including major cyber incidents. Issues addressed included the need to "bring the media into the fold" and what type of training could be useful to meet this need while leveraging existing courses where possible. Projects recommended included creation of a glossary of terms for general public use on emergency management and infrastructure security; inclusion of media in workshops, seminars and training events; and the creation of a short list of trusted subject matter experts to provide expertise to media. Other activities suggested included providing media training for all levels of employees, creation of a communications "tool-box" on how to inform the media of specific issues (e.g. cyber threats and attacks); and development of a web-based system to enable stakeholder personnel to get answers from experts on infrastructure security and general preparedness issues. Yet other ideas were to include a media group in NW WARN, and creation of a media guide on critical infrastructure interdependencies and cyber security challenges to help them understand the issues.

Other Participant Inputs

Meeting participants in their evaluations, and other BLUE CASCADES II attendees provided some additional ideas for projects, including holding a cross-border exercise in order to observe U.S. and Canadian interdependencies and related issues; criteria to determine critical assets, and better ways to protect and replace them if necessary; development of a region-wide system for mapping cyber and physical interdependencies and for creating modeling and simulation capabilities to analyze impacts, assess risk and determine cost-effective mitigation solutions. Also proposed was the creation of a Puget Sound Regional Partnership under the larger umbrella of the Pacific Northwest Partnership for Regional Infrastructure Security to provide a mechanism for stakeholders to meet, and to develop and monitor the Action Plan.

Initial Action Plan Projects

The following activities were selected from those ideas proposed in the respective Working Group discussions and other stakeholder inputs, as fairly well-defined, achievable by regional stakeholder organizations and cited by participants as particularly necessary. Funding for these projects is available or appears readily obtainable, an important consideration.

These projects are listed in the following categories: short-term/"low-hanging fruit" (six-months to one year/low cost); medium term (2 years); and long term (multi-year). It is envisioned that for the medium and longer-term projects, that at least the first six months will be spent defining project requirements. Because of the number of projects in the Plan, regional stakeholders will need to carefully prioritize them. Other projects will be added to the Action Plan as regional stakeholders undertake further discussions in subsequent meetings.

Short Term/"Low-Hanging fruit"

1. **NIMS Awareness Workshop** (for both public and private regional stakeholders)

2. **Expedited Clearance Process** (for private sector responders and staff of critical infrastructures. This is especially important to allow critical personnel (e.g., healthcare and utilities workers) to easily move across impacted geographic areas without being delayed by police barriers, etc.)

3. **BLUE CASCADES Exercise Program** (determine focus and schedule for future public-private targeted exercises to examine specific issues, e.g., roles and missions under certain scenarios; a cross-border exercise looking at U.S. and Canadian interdependencies and related issues)

4. **Puget Sound Region "Infrastructure Security Yellow Pages"** (template for stakeholders to use to provide information on stakeholder emergency and security points-of-contacts)

5. **Creation of a Puget Sound Regional Partnership for Infrastructure Security** (under the umbrella of the Pacific Northwest Partnership for Infrastructure Security, will continue process of building awareness and fostering stakeholder cooperation and provide input into critical infrastructure protection planning and disaster management efforts currently underway by state and local government in the region)

6. **Establishment of Cyber Security Council** (within the Puget Sound Regional Partnership, to address policy, legal and public disclosure issues; members would include industry, government, academic and nonprofit organizations that have established "pockets of excellence." The Council would be closely coordinated with other currently established regional cyber security organizations such as ISSA, Agora, etc.)

7. **"Partnering for Regional Preparedness" Web-based Resource** (will have different elements tailored to stakeholder needs, e.g., a dedicated cyber security link for the Cyber

Security Council; will be for information on best practices, regional capabilities, calendar of upcoming workshops, exercises, and other events)

8. **Inclusion of media in NW-WARN, workshops, seminars and training events**

9. **Infrastructure Security Handbook** (to provide general information on interdependencies and cyber security issues for broad public distribution)

10. **"Securing SCADA and Process Controls" Workshop"** (a "hands on" tutorial on threats, vulnerabilities and how to defend against them)

Medium Term

11. **Infrastructure Interdependencies Template** (for use by stakeholder organizations in-house and to enable mapping physical and cyber linkages on a regional basis)

12. **Information Sharing Protocols** (needed to support several of the Action Plan projects)

13. **Puget Sound Regional Information Sharing and Analysis Center** (will include an enhanced NW WARN and link to other existing information exchange and analysis capabilities in the region, including INFRAGARD; would track information on threats and cyber/physical attacks and assess trends, as well as other functions determined by stakeholders)

14. **Cyber Incident Threshold Criteria for Emergency Operation Center Stand up**

15. **Cyber Security and Incident Response Awareness Workshop** (develop formats customized for stakeholder personnel, media and general public)

16. **Integrated Incident Management System** (with Private Sector and other key organizations incorporated into NIMS)

17. **Cyber Security and First Aid Handbook** (for government and private sector organizations)

18. **Prolonged Power Emergencies Workshop** (develop formats customized for stakeholder personnel, media and general public)

19. **Region-wide Inventory and Assessment of Existing Physical and Cyber Disaster/Attack Preparedness Capabilities** (e.g., mechanisms, plans, procedures, methodologies, approaches, communications systems, sensors, and tools. Will provide a baseline of what has been done to avoid "recreating the wheel.")

20. **Emergency Backup Communications Systems Inventory and Assessment**

21. **Model Business Continuity Plan/Continuity of Operations Workshop** (for small and medium organizations, that includes interdependencies)

22. **Disaster Management Resource Inventory** (database of public and private sector resources available for response and recovery, including subject matter and technical experts, manpower, equipment and services, including information on reimbursement process).

23. **Critical Personnel Certification Process** (for travel of critical personnel across state and national borders during emergencies)

24. **Risk Communications Tool-box** (guidelines, procedures, and information to facilitate effective communication of pertinent, all hazards disaster-related information to the public and media; will include a glossary of common terms)

Long Term

25. **Decision Support System for Regional Infrastructure Security** (pilot project with DHS/S&T and Canadian federal government)

26. **Interdependencies Database and Analysis System** (pilot project with DHS/S&T and Canada; region-wide system for mapping, visualizing and analyzing cyber and physical interdependencies—may be virtual and will require development of procedures to handle security, legal and liability issues)

27. **Regional Infrastructure Security Plan** (focused on interdependencies and comprehensive in focus—all regional jurisdictions and all hazards; will incorporate results of Action Plan projects and be coordinated with and support the Regional Disaster Plan already in place, as well as other local and state plans).

Action Plan Implementation and Other BLUE CASCADES II Follow-On Activities

The preceding list of projects identified in the Action Plan, as previously noted, is only the first small step towards an on-going program of cost-effective activities that meet the overall objectives of the regional stakeholders. Developing a disaster-resilient region is a difficult task, made all the more daunting by limited understanding of infrastructure interdependencies and dearth of analytic capabilities to assess associated vulnerabilities and disruption impacts. While undertaking these initial Action Plan projects will be a good start, it is just the beginning of a planning and implementation process that will require setting flexible priorities that allow for other projects to be undertaken if funding becomes available or for other compelling reasons.

The Action Plan is meant to be dynamic and risk-based, expanding and changing consistent with regional stakeholder needs and interests, and incorporating lessons learned from other regional in the U.S. and from other nations from physical and cyber events. Most important,

the Action Plan is not a stand-alone effort but meant to be incorporated into federal, state and local government preparedness planning and to build upon existing capabilities.

The next step for regional stakeholders will be to prioritize and further develop these projects by defining requirements, selecting lead organizations for each effort, and determining the funding needed. This task, depending on the project involved, could be the responsibility of a working group, committee or task force of volunteers or may be an already established mechanism or government agency. Those working on each project will be responsible for devising the project schedule for meetings and milestones.

Looking Toward a Regional "Governance Structure". Clearly, to make meaningful progress, including securing funding and conducting project oversight, there is utility in "institutionalizing" in some way these collaborative preparedness activities. Projects could be undertaken on an *ad hoc* basis, with some taken under the wing of county, state and federal agencies, while others could be facilitated by PNWER or other appropriate organizations. Still others that require public and private collaboration may be developed through cooperative research and development agreements (CRADAs) that are negotiated by the participants.

Whatever the case--there must be a means for regional stakeholders to keep apprised and contribute to these projects as they are implemented. Many BLUE CASCADES II participants in their evaluations of both the exercise and the Action Planning meeting expressed the desire to continue convening in partnership to enhance regional readiness. Given this, it would be at a minimum useful to create within the Pacific Northwest Partnership a Puget Sound Partnership for Regional Infrastructure Security which could meet quarterly to receive reports from project leaders on progress towards implementation and to review and revise the Action Plan as necessary. The Puget Sound Partnership would continue to hold workshops and exercises to test progress made and uncover additional preparedness needs.

Moving Forward to Implementation. The biggest challenge facing stakeholders in undertaking the activities in the Action Plan will be to maintain the momentum needed to continue the BLUE CASCADES process. This means they must develop the necessary focus, flexibility, follow-through, fortitude and vision. Implementation will necessitate defining requirements, including program management and securing funding and technical expertise. Certain agencies and organizations will need to step up to the plate to take lead roles for the projects. There also needs to be a concerted effort to expand stakeholder involvement to organizations that have not been included in the BLUE CASCADES process to date. As one meeting attendee noted, "We are still participating with a narrow segment of the public/private sectors. Until we broaden the appreciation of the issues, we will not reach our goals."

Maintaining momentum will be a tall order, especially given that most public and private stakeholders are stretched thin with existing commitments and meetings. A number of Action Plan Meeting participants pointed this out. One state official emphasized the need to make use of existing organizations and relationships, but with the understanding that limited time and resources of personnel may make progress "…not as swift as some would like."

In the end, progress towards a disaster-resilient region will depend on the willingness of regional stakeholders to proactively move forward on implementation, and also enlightened and enthusiastic leadership from government and private sector leaders. Such leadership is essential, because Action Plan activities will be undertaken largely through existing state, local, and private sector mechanisms, with support, including technical assistance, from the federal government.

Appendix

BLUE CASCADES II RECOMMENDATIONS

Understanding Interdependencies (Cyber and Physical)

1. Using existing approaches and systems where possible, develop a collaborative, public-private sector initiative to identify and map regional interdependencies and develop the modeling and simulation tools that can analyze linkages, assess impacts of disruptions, ascertain preparedness gaps, and determine cost-effective mitigation measures.

2. Consider undertaking a collaborative pilot project involving organizations that rely on supply chains and computer systems to monitor and track products, cargo or passengers to develop the ability to analyze both the effects of disruptions on supply chains and the utility of mitigation options.

3. Develop criteria to enable stakeholders to better determine when a significant cyber attack is underway rather than just a nuisance incident.

4. Encourage organizations to integrate their emergency management, physical and cyber security and incident response activities and personnel to provide a comprehensive approach to disaster preparedness.

5. Develop a tutorial to educate personnel of regional stakeholders on: Develop a tutorial to educate personnel of regional stakeholders on:
    - The impacts of electric power and outages, including rolling blackouts and power surges on infrastructures, as well as other types of outages;
    - How to address SCADA/process control systems and related cyber threat, vulnerability, and mitigation issues.

Cooperation and Coordination

6. Create a regional Cyber Security Council within the Partnership for Regional Infrastructure Security to foster collaboration and to establish cyber emergency response and recovery protocols. This Council should coordinate and interact with other regional cyber security entities, such as INFRAGARD and AGORA, to ensure its activities take into account other regional cyber security efforts.

7. Develop a regional cyber emergency response/recovery plan that includes notification procedures and threshold criteria for standing up EOCs for cyber attacks.

8. Develop a region-wide "yellow-pages" of points-of-contact for disaster preparedness for regional stakeholders and determine means to keep it up-to-date. Leverage existing contact

lists and mechanisms such as NW-WARN for this purpose. Distribute the yellow pages in hard copy and digital format.

9. Develop a model continuity of operations plan for small and medium businesses and organizations that focuses on interdependencies and cyber disruptions/ attacks.

10. Develop cyber alert and warning procedures and checklists.

11. Undertake cyber vulnerability assessments of regional EOCs and other emergency response centers that can help identify cost-effective mitigation strategies to improve survivability and redundancy of IT and communication systems.

12. Create and conduct a series of seminars/ workshops to expand general knowledge of cyber threats, attacks, disruptions, impacts and response and recovery.

13. Work with the Department of Homeland Security and interested businesses to develop a model continuity of operations plan framework for small and medium commercial enterprises and organizations that includes interdependencies and cyber incident response and recovery.

14. Hold targeted exercises and workshops to further explore regional interdependencies, including those that go beyond state and national borders. Also use these events to test current practices, including resorting to manual operations, as well as preparedness improvements to address physical and cyber events.

15. Conduct an interdependencies seminar or exercise to specifically examine U.S- Canadian cross-border disaster response issues and incorporate the lessons learned into bi-lateral discussions on cooperative activities to address vulnerabilities and facilitate response and recovery in regional emergencies.

16. Develop training scenarios in PowerPoint format that utilities can use for educating and training employees.

17. Develop a dictionary of terms and acronyms that includes cyber security terminology to begin building a common language that all stakeholders can understand.

Communications and Information Exchange

18. Develop guidelines that take into account legal and proprietary issues to instruct organizations on when, how, and whom to notify within law enforcement about serious cyber problems.

19. Explore ways to provide expedited federal security clearances to enable dissemination of threat and other classified information to those in key stakeholder organizations who have a "need-to-know.

20. Further develop NW WARN as a regional mechanism for alerts and for sharing information, and include cyber threats and attacks as a focus area. Ensure that cyber security officials of infrastructures and other interested organizations are included in NW WARN.

21. Explore establishing a regional Information Sharing and Analysis Center to enable key stakeholders to better exchange and assess physical and cyber threat-related information in a trusted environment.

22. Provide support to state efforts to develop an interoperable communications systems that will provide redundancy in situations where phones, cell phones, and Internet access are unavailable

Roles and Responsibilities

23. Develop a better understanding among stakeholders of the National Response Plan and the National Incident Management (NIMS) System and how regional unified command will operate during a cyber attack. Explore the feasibility of incorporating key private sector organizations into NIMS.

24. Develop a regional cyber incident response plan.

25. Encourage the federal government to identify a single point of contact within the U.S. Government to respond to cyber emergencies.

Resource Management

26. Encourage the state to take the lead in working with city, county, federal government, and other relevant organizations in developing a roadmap of roles and responsibilities and what emergency services they offer.

27. Leverage existing efforts to develop a regional resource management plan that includes the oversight of prioritization and allocation of equipment, supplies, and mission essential personnel in major emergencies.

28. Develop a certification program for maintenance, emergency medical, and other critical private sector personnel who will need to provide essential services in a regional emergency to enable them to travel unimpeded through security roadblocks or to cross into other jurisdictions. Provide law enforcement with necessary training as part of this program.

29. Investigate how military and broader DOD assets could be employed in the event of a regional disaster. Incorporate these assets into regional preparedness planning, and test use of these assets in future regional exercises.

Public Information and Education

30. Establish a Web-based information resource for regional stakeholders that can be used to provide useful data for stakeholders and to function as a coordination and scheduling mechanism for exercises, seminars, conferences and as a vehicle to provide a regional event schedule. This Web resource could be undertaken by the Partnership for Regional Infrastructure Security and linked with state and local disaster response Web pages.

31. Using existing training courses, develop a terrorist awareness tutorial tailored to employees of regional infrastructures and organizations.

32. Develop a training course for private and public sector employees, including community institutions, on what they need to do in major emergencies and to familiarize them with state and local plans and requirements.

33. Develop a training course for public information officers and media on physical and cyber threats and impacts and include them in future workshops and exercises.