DHS/DOJ Fusion Process Technical Assistance Program and Services

Global Justice Information Sharing Initiative
United States Department of Justice

# FUSION CENTER SPOTLIGHT

## Washington State Fusion Center and the Pacific Northwest Economic Region:

## Building a Critical Infrastructure/ Key resource Information Sharing Capability

### Washington State Fusion Center

The Washington State Fusion Center (WSFC) was established by Charter in May 2009. The WSFC is governed by an Executive Board, whose members include the Washington State Patrol Chief, Federal Bureau of Investigation Seattle Field Division Special Agent-In-Charge, Seattle Police Department Chief, King County Sheriff, U.S. Attorney Western Washington District, U.S. Attorney Eastern Washington District, Washington State Homeland Security Advisor, Washington Association of Sheriffs' and Police Chiefs' President, Washington Association of Sheriffs and Police Chiefs Eastern Washington Representative. The WSFC's mission is to support the public safety and homeland security missions of Federal, State, local, and tribal agencies and private sector entities by serving as the State's single fusion center; detecting, deterring and preventing terrorist attacks; detecting, deterring and preventing significant criminal activity; performing threat assessment and information management services, including supporting the protection of critical infrastructure and key resources; and providing support to all hazards preparation, planning, response, and recovery efforts. Active participants in the WSFC include Washington State Patrol, Seattle Police Department, King County Sheriff's Office, U.S. Department of Homeland Security (DHS) Intelligence and Analysis, Washington National Guard, Immigration and Customs Enforcement, and Transportation Security Administration.

### The Pacific Northwest Economic Region

The Pacific Northwest Economic Region (PNWER) is a statutory non-profit created by the states of Alaska, Washington, Oregon, Idaho, Montana and the Canadian provinces of British Columbia, Alberta, Saskatchewan, and the Yukon Territory. PNWER's purpose is to collaborate and address issues that impact the cross-border regional economy of the Pacific Northwest. To this end, PNWER worked with stakeholders to develop the Pacific Northwest Partnership for Regional Infrastructure Security in 2002, and within Washington State a Puget Sound Partnership focused on the greater Seattle region the following year. As part of the Partnership's collaborative activities, a cross sector regional information sharing system was established called Northwest Warning, Alert and Response Network (NW WARN). Currently, more than 2000 vetted public and private critical infrastructure stakeholders from across the Pacific Northwest are members of this system.

## Incorporating Critical Infrastructure into the Fusion System

**Background**

Beginning in 2007, the WSFC partnered with PNWER to engage key stakeholders in a process to incorporate critical infrastructure and key resources (CIKR) organizations and other essential service providers to an expanded fusion system that enables cross-sector, two-way sharing of information, situational awareness, and analysis. The Seattle UASI Region –consisting of King, Pierce and Snohomish Counties—was chosen as the pilot area for this initiative to utilize the stakeholder relationships already developed through the Puget Sound Partnership for Regional Infrastructure Security. After development and testing by stakeholders, the CIKR component will be expanded to enable cross-sector information sharing throughout the rest of the state.

**Process Overview**

During the past year, PNWER and WSFC staff polled hundreds of public and private sector regional stakeholder organizations through the use of surveys and stakeholder meetings to develop requirements for the CIKR component of the WSFC. Initial work on the pilot project began with a kick-off meeting on June 19, 2008, with interested regional stakeholders attending. At this meeting the participants learned how the WSFC operates and is organized so they could offer input regarding how to best serve the broader stakeholder community. Work Group members subsequently convened via conference calls on July 19, August 5, and August 18. A broader stakeholder meeting was then held on September 5, 2008 to determine Pilot Project requirements. An extensive number of activities were subsequently conducted to meet the Pilot Project goals, including:

- Creation and facilitation of a Regional Information Sharing and Analysis Requirements Subgroup that convened on a regular basis to develop goals and objectives, and achieve specific outcomes;
- Development of a comprehensive overview of stakeholder requirements based on hundreds of interviews, conference calls, a targeted survey with stakeholder-validated questions, and numerous in-person meetings;
- Process and analysis of more than 140 detailed responses to an in-depth survey on stakeholder expectations, needs, and requirements as it relates to an information sharing fusion system;
- Research on critical infrastructure information sharing practices, protocols, existing mechanisms, and other capabilities that could be leveraged to implement the initial operating environment of the information fusion system;
- Development of two major workshops to solicit stakeholder input and feedback;
- Preparation of summary reports to provide requirements of infrastructure stakeholders;
- Facilitation of conference calls to solicit additional input on recommendations on the development of the fusion system;
- Development of a comprehensive initial Baseline Inventory of existing Federal, State, local, and private sector information sharing capabilities;
- Facilitation of 10 stakeholder and subject matter expert discussions on CIKR information sharing, security requirements, existing mechanisms, and procedures (e.g., NWWARN, Constellation/ACAMS, PCII);
- Development, with stakeholder input, of Information Fusion System participant criteria;
- Preparation of briefings for high-level DHS and Director of National Intelligence officials on the progress of the project;
- Preparation of project status briefings for regional congressional leadership and staff;
- Organization of a workshop for regional legislators on the importance of cross-sector information sharing, the need for a regional fusion system, and project progress;
- Coordination of a meeting with regional state/provincial CIKR managers to highlight the project's importance and gain input on the integration of law enforcement and emergency management; and

- Incorporation of a regional cyber incident management pilot being developed by the City of Seattle and the University of WA in cooperation with DHS into the fusion system project.

**Fusion System Needs Assessment**

PNWER and WSFC staff created a survey designed to identify stakeholder expectations, needs, and requirements as it relates to information sharing fusion system. The following questions were used to solicit feedback from a large number of stakeholders, not just those available to attend meetings and conference calls, and thus make the CIKR component as useful as possible to the population it is meant to serve.

1. What primary infrastructure sector or group do you represent?

2. What kind of functions, products, and services would your organization want or expect from a Cross-Sector Information Fusion and Analysis System that provides two-way information sharing?

3. Is your organization part of a sector consortium (formal or informal) of organizations with similar services for the purpose of sharing information and coordinating on threats or emergencies?

3a. If yes, what is (are) the name(s) of the consortium(s)?
3b. If so, would your organization be interested in setting up such a sector consortium?

4. What are the priority information needs for your organization and sector?

5. If you would you like to become a member of the Information Sharing Work Group please provide your contact information below.

6. Below are general categories and sector-specific services and products that private, public, and other key stakeholders have identified as needed or needing to be shared. On a scale of 1-5 (with 5 being the most important) please rate the following system requirements in terms of usefulness to your organization:

A. System for One-Stop Shopping (integrates existing and new capabilities and mechanisms to enable two-way cross-sector information sharing and analysis for all-hazards threats and disasters)

B. Alert and warning information (a push-pull system that includes search capabilities focused on incidents, emergencies, threats--deliberate and all-hazards)

C. General two-way situational awareness (all-hazards) information sharing and analysis

D. Public Health-related emergency information

E. Transportation critical infrastructure disruption issues

F. Maritime-related critical infrastructure security and all-hazards concerns

G. Regional risk assessment information; i.e., consequence and sector/asset resilience analysis and interdependencies analysis to support decision-making – both pre-incident for preparedness purposes and during response and recovery

H. Sanitization of classified and other sensitive material (for System users and their customers)

I. Processing and vetting of security clearances (based on "need-to-know" and system user requirements)

J. Training and "best practice" information for regional security and resilience (focused on protection, prevention, and preparedness)

K. Legal agreements and MOUs for users to protect proprietary information

7. What information or feedback could your organization or sector provide the fusion center? How might this information be shared with others?

8. Do you have any other input or comments on the development of a cross sector information and analysis system?

**Process Results**

The following were identified as component priorities for the Washington State Fusion Center's new CIKR information sharing system based on survey responses:

- Notification of transportation infrastructure disruption issue;
- General alert and warning information; specifically, a push-pull system that includes search capabilities focused on incidents and emergencies, to include both deliberate and all-hazards threats;
- A system for one-stop shopping that integrates both existing and new mechanisms to enable two-way cross-sector information sharing and analysis for all-hazards threats and disasters;
- Two-way situational awareness (all-hazards) information sharing and analysis with GIS capability;
- Status report of impacts and potential impacts to all critical infrastructures.

Additionally, PNWER and WSFC staff compiled information sharing priorities as they relate to each specific sector. The following needs were identified during the regional meetings, conference calls, and via the survey.

***Agriculture and Food***

- Early notice of possible food related illnesses/agro-terrorism occurring in the region;
- Establishing a single point of communication for information resources/emergency guidance;
- Appropriate data dissemination to agencies with feedback;
- Access to a government agency with the ability to do analysis of credit card fraud and identify the groups involved;
- Access to a broad range of information from transportation to cyber incidents;

***Banking and Finance***

- Trusted emergency notifications to the sector before media is notified;
- Restoration of essential services timelines;
- Real time information during events or occurrences that could impact the financial sector's ability to respond — i.e., traffic, power, or weather;
- Specific updates regarding cyber incidents.

***Chemical***

- Notifications regarding site security and crimes in the vicinity.

**Commercial Facilities**

- Current and actionable information;
- Information regarding infrastructure availability, the potential duration of impact, especially regarding power, water, sewer, transportation, and communications.

***Communications***

- Cross-sector information and intelligence sharing;
- Overall status report of all the critical infrastructures;
- Information on critical cell tower locations for priority restoration;
- Identification of Emergency Operation Centers (EOC) locations;
- Direct contact with energy sector to have power outage information on cell towers.

***Critical Manufacturing***

- Status report on critical infrastructure in the event of a wide scale emergency (important because impacts to the supply chain can have detrimental effects on just-in-time inventories).

***Dams and Levees***

- Real time communications for coordination between multiple federal, state, local and private organizations;
- Emergency notification and status reports on infrastructure needs, status, location, importance (criticality), protection level;
- Clearing house of information and "shield" from media as part of the Joint Information Center (JIC);
- Information on the capabilities of adversaries specific to the Dam and Levee Sector;
- Capabilities/Intentions of adversaries across all sectors.

***Defense Industrial Base***

- Information on impacts to infrastructures, including water, transportation, and communications (considered useful to planning response and recovery);
- Mechanism to inform infrastructures and U.S. Department of Defense contractors and customers.

***Emergency Services***

- Current threat information on an all hazards situational awareness (hazard-specific), alerting and notifications;
- Mechanism for information sharing and coordination for response and restoration;
- Threat information, including probable targets and methods of attack, particularly regarding critical infrastructure that may be targeted either because of its risk or vulnerability to a terrorist attack or natural disaster;
- Intelligence information that focuses on local issues;
- Information on emergency medical ingress and egress routes during an event;
- Repository for healthcare provider registration and/or credential verification and current contact list of key responders within all disciplines;
- Mobile-accessible, password-protected, access-monitored website portal;
- Officer safety information and crime bulletins;

- Identifiers (including photos) for subjects, organizations, or groups associated with the threat report or any related criminal activity;
- Links to past bulletins and sites regarding terrorism;
- Information resource for nontraditional responders such as public and private schools, public works, and private business.

***Energy***

- Intelligence and threat support during exercises, events and incidents;
- Threat information and reporting of suspicious activity and follow-up on the reports;
- Non-terrorism related criminal activity, such as metals theft trends;
- Information sharing with other organizations;
- Briefings on current security and resilience issues;
- Location of power outages;
- Emergency energy needs from all critical infrastructures;
- Identification of critical facilities that require emergency power;
- Radiological assistance team requests;
- Terrorist threats to U.S. Department of Energy Facilities;
- Notification of transportation disruptions that could affect recovery efforts, e.g., road, rail, and air closures;
- Assessment of critical back-up capabilities: hospitals, police, fire, and telecommunications.

***Government Facilities***

- Information on cross-sector critical infrastructure concerns including interdependencies;
- Establishment of a “lead contact” for each specific critical infrastructure;
- Creation of a “warehouse of information” with names of firms and staff capable of providing plans, special software tools (e.g. HAZUS-MH skills), phone lists of agencies and utilities, service providers, etc.;
- Mechanism to expedite responder credentialing;
- Information sharing with sector and state Information Sharing and Analysis Centers (ISACs) and US-CERT for cyber attacks and disruptions;
- Database distribution and receipt of critical information;
- Warning and alerting of suspicious events;
- Event criticality ratings;
- Means for government facilities to interface with public to provide data on regional utility locations, and transportation networks, including bridges and power grids;
- Information on attacks against information systems that support transportation, public safety, utility and inter-government agency communications systems;
- General situational awareness bulletins;
- Portal for secure documents to be shared to vetted participants.

***Information Technology***

- Timely info on regional cyber security incidents, trends, tactics, and intelligence data;
- Sharing of defense tools and strategies;
- Access to data on utility outages and road closures to map them during an event;

- GIS database that is maintained and updated on a quarterly basis;
- Creation of standards for integrating and interfacing a variety of existing applications;
- Web-based, secure, two way communications;
- Alerts of physical security threats to key IT and communications facilities and supporting infrastructure.

***National Monuments and Icons***

- Site security and crimes in the vicinity related information;
- Date-specific intelligence, e.g., weather, traffic, or any possible threats impacting events such as sporting events or large gatherings of people.

***Nuclear Reactors, Materials and Waste***

- Site security and crimes in the vicinity related information.

***Postal and Shipping***

- Terror alerts, crime patterns, and current criminal activity;
- Anything that may affect businesses' ability to operate, e.g., road closures due to disasters, hazardous situations requiring the evacuation of employees, disruptions to shipping operations, etc.

***Public Health and Healthcare***

- Alert and warning concerning potential threats such as communicable diseases, bioterrorism, outbreaks, animal diseases, air quality, water contamination, etc. to public health;
- Dedicated fusion center analyst that understands public health issues who can share information within and across sectors.

***Transportation Systems***

- All hazard warning with analysis and reporting to allow advance planning;
- Training analysts (with security clearances) who can assist in the distribution of open source information for the rest of the sector;
- Critical Infrastructure status reports and updates;
- Pre-incident engagements/exercises;
- Best practices sharing;
- Advisories regarding strategy and capabilities;
- Resource needs updates;
- Criminal statistics;
- Threat and vulnerability assessments;
- Information regarding commercial vessel activity in Puget Sound during times of crisis when congestion or other restriction may result in delays;
- Data on resiliency and/or recovery of the marine transportation system;
- Information on port closure and resumption of operations;
- Portal for secure documents to be shared to vetted participants, including emergency response plans;
- Network for cross-sector collaboration;
- Cross-sector infrastructure interdependencies information.

***Water and Wastewater Sector***

- Potential or real threat warning, alert, and analysis;
- Resource management tool for response and recovery;
- Strike team training (both inter-agency and intra-agency) for fusion center personnel;
- Place for submittal of reports, summaries and assessments of all-hazard events;
- Coordination tool for city, county, and the FBI during a terrorist event;
- National Weather Service updates regarding extreme weather and natural disasters;
- Coordination of regional damage assessment information reporting.

### Development of the CIKR Component Concept of Operations

PNWER and Fusion Center staff utilized the results of these studies to develop an initial operating capability with a Concept of Operations (CONOPS) and Standard Operating Procedures. The CONOPS was presented to stakeholders in March for comment and then finalized. The CONOPSs outlined a CIKR capability which can disseminate alerts, warnings, notifications and other relevant analytic reports to an affected critical infrastructure or private sector organization, receive tips and leads from CIKR entities relevant to the center's all-hazards mission, provides for a secure cross-sector collaborative space, a critical infrastructure information database, CIKR sector-specific analytical resource group, analytical capability, customer feedback/reevaluation mechanism, and outreach and education for CIKR component members. The CONOPS also covers information collection requirements, information protection procedures (including PCII), a membership vetting and approval process, and information dissemination.

### Towards A State-Wide CIKR Information Sharing Component

With the CIKR component planning and requirements completed, the next steps are to continue initial system implementation with completion of procedures and mechanisms for information collection, analysis and production, and dissemination by mid-year. The CIKR Sector Specific Analytical Resource Group is being established, and the Pilot Information Sharing Platform based on NWWARN and exercise to tests the Pilot SOP and processes are also nearly completed. Training for CIKR participants and the initial Critical Infrastructure Liaison Program participants will also be finalized within the next few months.

### Opportunities and Challenges

The CIKR information sharing capability will enhance the relationship and communication between the Fusion Center and private sector, further improve understanding of infrastructure and interdependencies, ensure CIKR perspectives are considered in analysis, products, and services; and provide CIKR representatives training that ultimately results in a protection and response 'force multiplier', and a safer community. The capability also will support and improve preparedness, protection, planning, and response efforts across all levels of government and CIKR sectors, and provide leaders and CIKR decision makers more accurate situational awareness upon which to base emergency planning, preparedness, and response decisions.

At the same time, both WSFC and PNWER recognize there are continuing challenges that remain. Resources—staff, technical assistance, and funding, are severely limited. There are cultural, cross-discipline impediments. It is clear that public-private partnerships/coalitions play a key role in maintaining and improving a CIKR fusion system, but the challenge is how to ensure adequate CIKR membership representation. Also, there is the need to

**FOR MORE INFORMATION**

**If you require information regarding the Fusion Process Technical Assistance Program or assistance with the request process, please contact Kevin Saupp at kevin.saupp@dhs.gov or Patrick McCreary at james.p.mccreary@usdoj.gov.**

balance information sharing and protection, and to address expectations of stakeholders given resource and institutional constraints.  Lastly there is the overall challenge of assuring adaptability and sustainability of the CIKR information-sharing component within the Fusion Center.  WSFC, PNWER, and regional stakeholders remain committed to collaboratively address these challenges in the months ahead.