Around The Region In Homeland Security
April 2013

The Northwest Regional Technology Center (NWRTC) is a virtual resource center, operated by the Pacific Northwest National Laboratory (PNNL), to support regional preparedness, resiliency, response, and recovery. The center enables homeland security solutions for emergency responder communities and federal, state, and local stakeholders in the Northwest. This monthly newsletter summarizes activities related to homeland security in the region, and this issue highlights

- ➢ Cyber Summit: Tackling Critical Cyber Challenges
- ➢ 9-1-1 Awareness Month
- ➢ Comments Sought to Improve Cybersecurity Practices
- ➢ Upcoming Events

Cyber Summit: Tackling Critical Cyber Challenges

Cyber Summit: Briefings & Demonstration, jointly hosted by PNNL and the Snohomish County PUD, was held recently in Seattle, Washington. The Summit provided a venue for information sharing and education about cybersecurity concerns, advancements and resources important to Washington State stakeholders.

“Cybersecurity is important to everybody” said Ann Lesperance, deputy director of the NWRTC and Summit moderator. “This forum provides an opportunity to capitalize on and learn from our regional assets.”

Participants included

- Mike Smith, Senior Cyber Policy Advisor, DOE Office of Electricity Delivery & Energy Reliability
- Samara Moore, National Security Staff; Director, Critical Infrastructure, White House
- Troy Thompson, Cyber Account Manager, PNNL
- Benjamin Beberness, CIO, Snohomish County PUD
- Mike Hamilton, CISO, City of Seattle
- Philip Jones, WUTC and President, NARUC
- Lt. Col Welsh, General Daugherty and General Magonigle, all of the Washington State National Guard

A summary report from the Summit is currently being prepared, including briefings and demonstrations. To request a copy, email ann.lesperance@pnnl.gov.

Steve Klein, CEO Snohomish Public Utility District, Congresswoman Suzan DelBene and Mike Kluse PNNL Laboratory Director welcomed attendees to the well-attended event.

9-1-1 Awareness Month

April is National 9-1-1 Education Month, and public organizations are working to educate the community about the appropriate use of this emergency service. In response, members of the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) First Responder Resource Group (FRRG) shared their experiences, best practices, and lessons learned related to 9-1-1. One example is related to cybersecurity challenges.

Cybersecurity is becoming an increasingly important issue for public safety answering points (PSAPs) as they are becoming more connected with services, networks and online systems. One example provided by Jay English, Director of Communications Center and 9-1-1 Services, Association of Public-Safety Communications Officials (APCO) International, is a recent attack on The Louisiana Fusion Center. After contacting DHS with what at first appeared to be a few isolated attacks, cyber security resources were quickly mobilized. Within days, several agencies had joined together to form a single point of contact for Telephony Denial of Service (TDoS) attack incident reporting which has netted reports of hundreds of additional attacks.

Seeing a need for proactive planning, the Best Practices Checklist for Denial of Service Attacks Against 9-1-1 Centers was created by a group of federal authorities, public safety representatives, and commercial service providers. The document aids PSAPs in developing strategies for mitigating risk and for approaches to dealing with a TDoS incident should one occur.

To view the original article, visit http://www.firstresponder.gov/Pages/FRPDFArticles.aspx?Article=143.

Comments Sought to Improve Cybersecurity Practices

The Commerce Department is seeking industry ideas about ways to incentivize critical infrastructure owners and operators to adopt cybersecurity measures.

Specifically, the Secretary of Homeland Security is seeking suggestions to promote the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. Feedback will be used to inform recommendations for critical infrastructure owners and, possibly, to broader U.S. industry. Full text of the notice *Incentives to Adopt Improved Cybersecurity Practices* is available on the Federal Register.

Comments are due on or before April 29, 2013.

Upcoming Events

April 29, 2013
Developing and Sustaining Regional Collaboration
DPSST, Salem, OR

May 14, 2013
Community Points of Distribution Manager's Course
Yakima County, WA

Around the Region in Homeland Security is a monthly report from PNNL's Northwest Regional Technology Center for Homeland Security. For more information, contact Director Steve Stein at steve.stein@pnnl.gov or 206-528-3340, Deputy Director Ryan Eddy at ryan.eddy@pnnl.gov or 509-372-6622, or Deputy Director Regional Programs Ann Lesperance at ann.lesperance@pnnl.gov or 206-528-3223, or see the website at http://nwrtc.pnnl.gov.
PNNL-SA-95167

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965