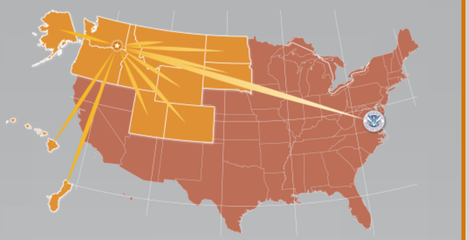
NORTHWEST REGIONAL TECHNOLOGY CENTER
for Homeland Security

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



UPCOMING EVENTS

- Nov. 2015 – Critical Infrastructure Security & Resilience Month
- Nov. 17-19, 2015 – Emergency Preparedness and Business Continuity Conference, Vancouver, BC
- Dec. 1-4, 2015 – 2015 National Healthcare Coalition Preparedness Conference, San Diego, CA
- Dec. 10, 2015 – Building Resilience through Public-Private Partnerships Conference, New Orleans, LA

CONTACT

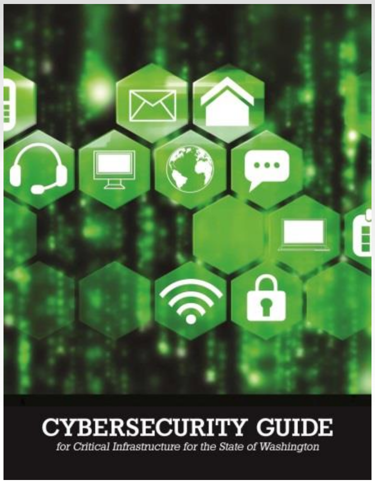
- Want to know more? Visit us on the web at http://nwrtc.pnnl.gov
- Contact the NWRTC with questions and comments at nwrtc@pnnl.gov.

AROUND THE REGION IN HOMELAND SECURITY

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.

CYBERSECURITY GUIDE STRENGTHENS WASHINGTON'S CYBER POSTURE

In September, the Energy Sector Cybersecurity Working Group in Washington State released the "Cybersecurity Guide for Critical Infrastructure for the State of Washington," which identifies the most current best cyber practices and tools for protecting critical infrastructure entities throughout the state. The guide is based on the National Institute of Standards and Technology framework and designed to provide cybersecurity and resource information for entities operating critical infrastructure that often lack the resources for comprehensive cyber defense capabilities.



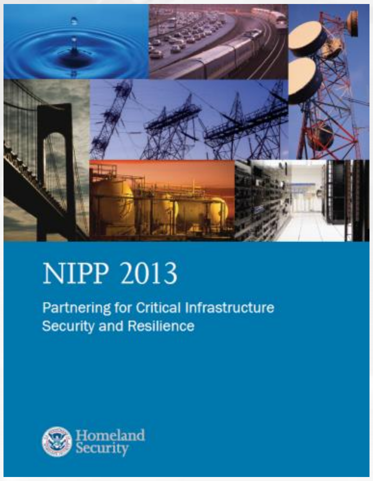
CYBERSECURITY GUIDE
for Critical Infrastructure for the State of Washington

Cybersecurity Guide for Critical Infrastructure of Washington State

"The intention of this guide is to provide a building block for small to mid-size companies to become more secure, specifically to assist them with their cybersecurity strategy and posture. Currently, power and water trade associations are using this guide as a free resource for their members," said Jessica Matlock, Director of Government Relations for Snohomish County Public Utility District (SnoPUD).

The guide was produced by the Energy Sector Cybersecurity Working Group, a collaborative effort between the Washington State Utilities and Transportation Commission, Washington State National Guard, Washington State Emergency Management Division, State of Washington Office of the Chief information Officer, PNNL, and SnoPUD. To learn more about Washington cybersecurity, a PDF version of the guide and press release are available online.

PROTECTING CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE


NIPP 2013

Partnering for Critical Infrastructure Security and Resilience

Homeland Security

DHS National Infrastructure Protection Plan

November is Critical Infrastructure Security and Resilience month, aimed at raising awareness and appreciation of critical infrastructure protection and of the nationwide commitment to keep critical infrastructure and communities safe and secure. This month, the Department of Homeland Security (DHS) is specifically focusing on raising awareness of the 2015 Sector Specific Plans, which supplement the National Infrastructure Protection Plan and describe the operating conditions and risk landscape within the 16 critical infrastructure sectors (chemical, dams, emergency services, energy, etc.).

To learn more about the nationwide efforts to protect the nation's critical infrastructure, visit http://www.dhs.gov/critical-infrastructure-security-resilience-month. The site provides a variety of ways to get involved as well as resources such as a Critical Infrastructure Security and Resilience Month Toolkit and fact sheet.

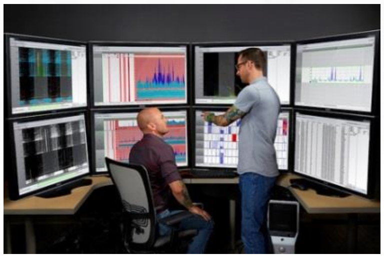
FRIENDLY HACK TESTS UTILITY'S CYBER DEFENSES

A team of cybersecurity professionals from the Washington State National Guard and a series of industry experts recently tested the cyber defenses of SnoPUD. The friendly but life-like hack featured a realistic-looking work email disseminated to employees. A few recipients opened the message, which unloaded the illicit content. Participants said the exercise demonstrated that, while a utility may embrace a range of cyber defenses, employee cyber awareness can often be the easiest opportunity for a cyberattack.

Both SnoPUD and the Washington State National Guard are part of the Energy Sector Cybersecurity Working Group in Washington State that recently published the Cybersecurity Guide for Critical Infrastructure for the State of Washington. These activities were born out of annual cybersecurity summits sponsored by SnoPUD, PNNL, and others. The outcomes from the summit are available in the Pacific Northwest Cyber Summit Briefings and Demonstration Summary Report available on the NWRTC web site.

For more information, read the Energy & Environmental Publishing article "Friendly hackers break into a utility and make a point" by reporter Peter Behr.

PNNL TAPPED TO SUPPORT DHS PROGRAM



PNNL has been named a supporting laboratory to the National Infrastructure Simulation and Analysis Center (NISAC). NISAC is a DHS program that addresses the potential vulnerabilities and consequences of disruption of our nation's critical infrastructure, such as the electric grid. NISAC coordinates scientific computational capabilities, as well as modeling and analysis expertise to discover relationships and develop insights about infrastructure vulnerabilities in the case of natural disasters, and both intentional and accidental manmade events. PNNL will contribute advanced computer modeling and simulation capabilities to look at the dependencies, interdependencies, vulnerabilities, and complexities of important critical infrastructure sectors such as dams, water, transportation, energy, and information technology. For more information, a press release is available online.

For more information, contact NWRTC Director Ann Lesperance at ann.lesperance@pnnl.gov or 206-528-3223, Deputy Director Ryan Eddy at ryan.eddy@pnnl.gov or 509-372-6622, Technical Advisor Steve Stein at steve.stein@pnnl.gov or 206-528-3340, or visit us online at http://nwrtc.pnnl.gov.