OPPORTUNITIES
Events current at time of publication. Have a virtual resource or event to share? Email us!

- March 7-9 – Critical Infrastructure Protection and Resilience Americas
- April 4-6 – Partners in Emergency Preparedness 2023 Conference
- April 4-7 – Association of County and City Information Systems Spring 2023 Conference
- July 24-27 – National Homeland Security Conference

CONTACT
Want to know more? Visit us at pnnl.gov/projects/nwrtc. 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 Pacific Northwest National Laboratory (PNNL), to support regional preparedness, resilience, response, and recovery. The center enables homeland security solutions for emergency responder communities and federal, state, and local stakeholders in the Northwest.

HAPPY NEW YEAR AND WELCOME TO 2023!

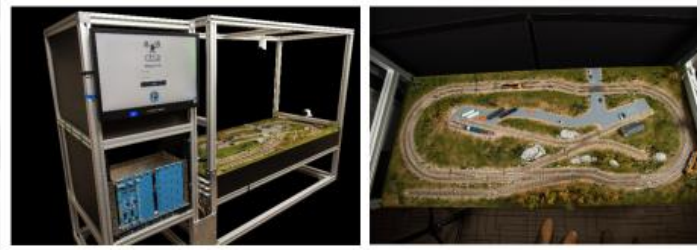
To kick off 2023, I would like to extend a resounding thank you to all of our readers for your continued support to our center and to the partnerships and opportunities we build.

We are ringing in this new year following several successful outreach events in 2022. In May, our NWRTC Virtual Summit convened more than 40 representatives from 11 states and the Territory of Guam with senior leaders from the Department of Homeland Security (DHS). This was our first summit since 2008, and it was an exciting opportunity to hear from so many states about their priorities. The summit was an invigorating refresher as to why our center exists and how we can use it to better connect our science and technology with homeland security stakeholders in the Pacific Northwest and beyond.

In September, the Washington State Cyber Incident Response Summit convened 40 key decision makers and stakeholders from across the state to discuss strategies and pilot a collaborative approach to improve cyber incident response readiness within Washington. The small working groups identified a number of lessons learned, best practices, and opportunities to be explored in the future.

These events are just a snapshot of the connections being made between our NWRTC team and the first responder, public safety, and emergency management community. They set the stage for what I hope will be a productive new year! If you are interested in connecting, attending future events, or learning about PNNL science and technology, please reach out!

Ann Lesperance
NWRTC Director, PNNL



PNNL's rail test environment will be designed to help rail industry experts prepare for potential cyberattacks against rail infrastructure.

TEST ENVIRONMENTS HELP SECURE TRANSPORTATION INFRASTRUCTURE

Together with the Cybersecurity and Infrastructure Security Agency (CISA), the DHS Science and Technology Directorate (S&T) is working with a multi-agency team, including PNNL and Idaho National Laboratory (INL), and other government and private stakeholders to design and implement two state-of-the-art training tools focused on automotive and rail test environments. These will both be a part of CISA's Control Environment Laboratory Resource test environment.

In this effort, PNNL is working with rail transportation subject matter experts to develop a test environment that will provide CISA, other internet security professionals, and rail operators and manufacturers with a tool to better understand, manage, and reduce the possibility and effects of successful hacking and cyber-physical attacks aimed at trains and associated infrastructure.

"Our test environment will model freight line operations; emulate traffic control, train control, and train communications systems; and serve as an educational platform for rail industry IT staff, manufacturers, and operators to prepare for real-world cyberattacks," explained PNNL cybersecurity research scientist Thomas Edgar.

INL's automotive test bed will target a better understanding of electric semi-autonomous vehicles and the ways that their systems and components can potentially affect other drivers and vehicles.

Read the S&T feature article to learn more.

TRAINING NEXT-GENERATION CYBER GUARDIANS

PISCES
Public Infrastructure Security Cyber Education System

Because not a day goes by without a cyber incident in the news, one Washington State-based nonprofit organization is here to help. The Public Infrastructure Security Cyber Education System (PISCES) provides undergraduate students with supervised experiences to serve as entry-level cyber analysts. In the *Domestic Preparedness* commentary "Training the Next Generation of Cyber Guardians," PISCES founder and former NWRTC Director Steven Stein shares how this one-of-a-kind program is delivering a reliable, high-quality pipeline of entry-level cyber analysts with operational experience to address the shortage of cyber professionals, while simultaneously providing a level of monitoring to critical infrastructure networks.

Since its founding in 2017, PISCES has worked with DHS and PNNL to establish, develop, and grow this nonprofit into a nationwide program. With 10 academic institutions and more than 20 communities sharing data, PISCES provides 300-400 students per year with this critical experience. Learn more at https://pisces-intl.org/.

PLANNING FRAMEWORK AIDS INFRASTRUCTURE RESILIENCE

CISA has released an updated Infrastructure Resilience Planning Framework to help state, local, tribal, and territorial planners better protect infrastructure. The framework helps partners to incorporate critical infrastructure resilience considerations into planning activities and can be used to support capital improvement plans, hazard mitigation plans, and other planning documents, as well as funding requests. Read more.

For more information, contact Director Ann Lesperance (ann.lesperance@pnnl.gov | (206) 528-3223) or Deputy Director Richard Ozanich (richard.ozanich@pnnl.gov | (509) 375-4586) or visit pnnl.gov/projects/nwrtc.
PNNL-SA-180901