



NWRTC

Northwest Regional
Technology Center
@PNNL



Pacific Northwest
NATIONAL LABORATORY

OPPORTUNITIES

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

- July 20-24 – [Pacific NorthWest Economic Region 34th Annual Summit](#)
- July 27-30 – [Association of Public Safety Communications Officials Annual Conference and Expo](#)
- August 25-28 – [National Homeland Security Conference](#)
- October 9-12 – [National Emergency Management Association 2025 Annual Forum](#)
- October 18-21 – [International Association of Chiefs of Police Annual Conference](#)
- October 29-30 – [Partners in Emergency Preparedness](#)

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), that supports 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.

DATABASE TRACKS WILDFIRE MITIGATION PLANS NATIONWIDE

To aid in wildfire preparedness, PNNL has released a publicly accessible [online database of wildfire mitigation plans](#). The new resource offers a centralized, searchable collection of more than 400 publicly available wildfire mitigation plans developed by 170 utilities across 19 U.S. states. These plans span 2019 through 2028 and provide a broad overview of how utilities are preparing for wildfire risk.



The database is funded by the Department of Energy's Grid Deployment Office and is part of a larger research program focused on establishing credible industry metrics for assessing and mitigating wildfire risk.

The database, now live and available for public use, was built to support electric utilities, state governments, policymakers, and regulators in understanding and improving [wildfire risk and resilience](#) strategies. It comes at a time when wildfires are becoming more frequent and severe, posing increasing threats to power infrastructure, public safety, and taxpayer dollars.

PNNL encourages utilities, agencies, and other stakeholders to [explore the database](#), contribute to the case studies, and participate in upcoming workshops and interviews. Together, these initiatives aim to support smarter, more coordinated wildfire mitigation efforts and pave the way toward a more resilient energy future.

Read the [PNNL article](#) to learn more.



MODELING THE FUTURE OF AIRPORT SECURITY

The number of air travelers is rising each year, which poses capacity challenges for many airports in terms of performing passenger screening and maintaining the resources and space needed to manage potential security risks. To help airports better manage these risks while still enhancing the passenger experience, a research team led by PNNL developed the Aviation Security Screening Optimizer for Risk and Throughput (ASSORT) risk model. ASSORT's methodology in assessing risk-based approaches for passenger screening and checkpoint operations was the focus of a paper recently [published in the *Journal of Transportation Security*](#).



Speaking to the benefits of ASSORT, as outlined in the paper, PNNL's [Robert Brigantic](#), a chief operations research scientist and ASSORT principal investigator, said, "Our model provides a means to quantify risk for different threat scenarios and then computes the overall risk to the checkpoint, aircraft, and airport by different traveler types. For airports, this could mean quicker and more accurate assessments of the trade-offs between the overall risk associated with checkpoints and the throughput rate of passengers screened."

ASSORT aligns with PNNL's decades-long history of delivering science and technology for aviation security, including its [award-winning millimeter-wave technology](#). ASSORT is based on and extends PNNL's [Airport Risk Assessment Model](#) risk formulation as well as its scoring guide, which applies definitions, scoring criteria, and methodologies from the Department of Homeland Security and the U.S. Coast Guard to the process of scoring risk parameters.

Read the [PNNL staff accomplishment](#) to learn more.

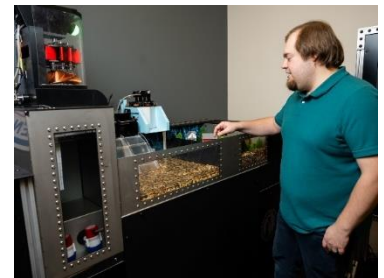
FIGHTING CYBER THREATS AT U.S. HYDROPOWER SYSTEMS

Experts at PNNL are developing novel approaches to protect, detect, and recover from potential cyberattacks at the hydroelectric facilities that produce nearly 6 percent of the nation's total electricity—and more than 60 percent of the power generated in the state of Washington. Researchers are combining their knowledge of the hydropower system and expertise in cybersecurity to secure the operational technology of the nation's hydropower fleet.

To make it easier for operators who may need to respond to and recover from a cyber incident, researchers assembled and integrated guidance from several agencies and created a cyber-physical framework and roadmap for the nation's entire fleet. They also prepared and shared a step-by-step desk guide for navigating a cyberattack.

In a separate effort to train cybersecurity professionals working on critical infrastructure, PNNL researchers developed a [series of test platforms](#). These platforms, often referred to as skids, are scaled-down, functional models that enable realistic exercises without putting real infrastructure at risk.

The hydropower skid and associated training scenarios were designed with input from regional hydropower plant operators, including Spokane-based Avista Corporation and Grant County Public Utility District.



Read the [PNNL director's column](#) and [check out this video](#) to learn more.