

INL News Release
FOR IMMEDIATE RELEASE
Aug. 30, 2012

NEWS MEDIA CONTACTS:

Misty Benjamin, 208-526-5940, misty.benjamin@inl.gov
Ethan Huffman, 208-526-0660, ethan.huffman@inl.gov

Cybersecurity tool suite demonstrated this week

IDAHO FALLS — The future of cybersecurity being shaped at Idaho National Laboratory is on display for energy industry stakeholders and U.S. Department of Energy officials this week.

The lab is demonstrating a suite of cybersecurity tools that provides situational awareness of networks and control systems. Such awareness enables an energy utility to further safeguard its systems from cyberattack.

"We're trying to help people better understand their computer networks so they can better protect them," said Robert Erbes, the INL cybersecurity researcher leading the demonstration.

In some ways, a utility's computer networks resemble the body's central nervous system. They send critical information throughout the company, enable communication between diverse elements, and connect to supervisory data and control systems that help run the company's physical equipment.

INL has built an international reputation leading control systems cybersecurity advances.

DOE's Office of Electricity Delivery & Energy Reliability (DOE-OE) provides funding to help improve the cybersecurity of the nation's control systems. Two years ago, the office's Cybersecurity for Energy Delivery Systems program funded a project at INL to develop a suite of tools to provide improved overall situation awareness of control and sensor network systems. A group of energy industry stakeholders along with DOE representatives will see the results during this week's demonstration.

The interoperative tool suite consists of applications ranging from concrete, implementable ideas to academic-based research demonstrations.

Among the tools being demonstrated is the [Sophia situational awareness software](#). It passively observes network communications, providing both real-time and historical records of those communications. [Sophia](#) can also be configured to automatically detect unusual activity that may present a security concern. Like the other tools INL is demonstrating, it provides all of its information for human operators to evaluate.

"The INL research team is aiming to provide situational awareness so the human can make the decision about how to respond or react," said Erbes.

The other tools that are part of the interoperability demonstration this week are Intelligent Cyber Sensor, Data Fusion and the Net Access Policy Tool (NetAPT), which was developed by the University of Illinois at Urbana-Champaign. The INL project team also will be demonstrating five additional cybersecurity research projects.

INL is one of the DOE's 10 multiprogram national laboratories. The laboratory performs work in each of DOE's strategic goal areas: energy, national security, science and environment. INL is the nation's leading center for nuclear energy research and development. Day-to-day management and operation of the laboratory is the responsibility of Battelle Energy Alliance.

Find INL news and feature stories at www.inl.gov. Follow @INL on Twitter or visit our Facebook page at www.facebook.com/IdahoNationalLaboratory.

—INL-12-025—

[News Release Archive](#)