

Experts from across NNSA feel the heat in LLNL cyber exercise

09/21/2011



A cyber security exercise hosted by the Laboratory last week brought together the National Nuclear Security Administration's elite cyber responders.

Photo by Jacqueline McBride/LLNL

Out of the FIRE and into the INFERNO was the idea behind a cyber security exercise hosted by the Laboratory last week that brought together the National Nuclear Security Administration's elite cyber responders.

In a first exercise of its kind, cyber security responders from NNSA sites around the country gathered for three days of cyber combat to repel a would-be intruder -- the kind of attacks NNSA/DOE institutions see with increasing frequency.

Cyber attacks often target multiple institutions within DOE and NNSA (not to mention other federal agencies), necessitating a coordinated response, according to Neale Pickett, the Los Alamos National Laboratory (LANL) cyber security specialist who organized the exercise hosted by Livermore. "There's increasing recognition among the NNSA sites that we can no longer continue to operate as islands."

Called Tracer INFERNO, the exercise was based on an attack experienced earlier this year by a number of DOE/NNSA labs, and is a play on the Tracer Forensic Individual Response Event (FIRE) Pickett has organized at LANL, a workshop/competition that focuses more on internal team building and training for people new to the field.

Because it was based on a real incident and responders wanted to turn up the heat on the challenge, last week's exercise at LLNL was called an Intensive Network Forensic Exercise on Real Network Operations, or INFERNO for short. Conceived for NNSA's elite cyber responders, "Tracer Inferno is a more advanced event focused on building relationships across the complex,"

Pickett said.

"There's a lot of expertise at each of the labs," he said. "What is going to happen as a result of this exercise is that people are going to know each other and have experience working together. We will be better able to respond to future threats."

"These kind of cyber attacks are happening more frequently," said Matt Myrick, a senior cyber security engineer in LLNL's Cyber Security Program. "The more we talk among ourselves, the more we see patterns and the more we can share information across NNSA."

Participating in Tracer Inferno were 26 people from NNSA institutions, including: Y12 (Oak Ridge, Tenn.); LANL; Sandia National Laboratories; Savannah River; Pantex; the Kansas City Plant; NNSA's Information Assurance Response Center; and Livermore.

NNSA recognizes the need to build a complex-wide cyber defense capability, Pickett said, noting that the exercise is a relatively inexpensive way to build such a response capability. "Everyone thinks it's a good idea," Myrick said. "Through exercises such as this we can develop a multi-institutional team of incident responders and we can have a pool of people to draw from. This is an idea that is now being formalized."

In a related event in July, the Laboratory hosted a cyber defenders workshop for students. See [Newsline](#).