

## **New DHS Cyber-Security Working Group Links Agencies**

Mar 9, 2009, By Hilton Collins

The U.S. Department of Homeland Security has created a collaborative venture for public- and private-sector organizations in order to nip problems in the bud that are associated with industrial control systems -- at least the ones that can be nipped by computer.

The Control Systems Security Program (CSSP), offered by the Department of Homeland Security's National Cybersecurity Division, has created the Industrial Control Systems Joint Working Group (ICSJWG) to allow the federal government to work with vendors and state and local agencies to address high-tech issues in their operations. The Department of Homeland Security issued a press release in February 2009 about the work group, but the group had already been established earlier in January.

"Basically what we focus on in the industrial control systems, or ICS community -- it's that connection between the cyber-world, or virtual world, and the real world," explained Sean McGurk, the director of control systems security in the National Cyber Security Division. "Essentially it's everything that you see in the real world that is controlled by a computer, for all intents and purposes."

This includes systems that run aquariums and zoos, people movers, roller coasters, data centers, power generation and distribution at nuclear facilities, chemical processing and manufacturing, oil and natural gas pipeline systems, heating and air conditioning -most of what anyone could think of in the systems-control arena.

Because so many of these systems are computerized, they're also vulnerable to security holes.

"With the advent and the induction of common information technology architecture into the process, all of those same bugs and vulnerabilities associated with information technology could now potentially have an impact in the industrial control space," McGurk said.

### **DHS Cyber-Security Group Spans Government Levels**

The federal government plans for the ICSJWG to be a means for organizations that operate and manufacture these systems to keep bugs under control. The group is chartered by the Critical Infrastructure Partnership Advisory Council, established by the Department of Homeland Security to facilitate coordination between federal and nonfederal infrastructure control programs.

The ICSJWG spans 18 critical infrastructure and key resources sectors, such as agriculture and food, banking and finance, and nuclear reactors.

The federal government also plans for the work of the organizations in the ICSJWG to align with goals set in the 2009 National Infrastructure Protection Plan (NIPP), a document published by the Department of Homeland Security. The NIPP outlines a unifying structure for organizations in all 18 sectors to adhere to in order to protect their systems and resources.

"One of the key elements of this working group will be information sharing and analysis so that we can provide actionable information so that facilities can become more secure when there is a potential risk associated with their operating systems," McGurk said.

The ICSJWG takes over where the Process Control System Forum (PCSF) left off. The DHS' Directorate for Science and Technology Division created the PCSF in 2005 to develop a methodology to change process-control. McGurk said that the ICSJWG is an evolution of the PCSF that will take public- and private-sector

collaboration to the next level.

The ICSJWG will meet several times each year, via in-person and virtual get-togethers, either by phone bridge or other means.