NIST Process Control Security Requirements Forum (PCSRF)

The National Institute of Standards and Technology (NIST) is working with process control end users, vendors and integrators to improve the IT security of networked digital control systems used in industrial applications. The widespread use of IT for remote monitoring and control of the electric power system and for controlling industrial processes in the oil and gas, water, chemical, pharmaceutical, food and beverage, pulp and paper, and other industries, has unintentionally introduced security vulnerabilities. These systems are time critical and were designed to maximize performance, reliability and safety. Security has not been a significant consideration because these systems were often air-gapped from any other network and based on proprietary hardware and protocols. This has been called security through obscurity. But today, these process control systems are often connected to the business networks to allow business people to make decisions and use commercial of the shelf products and open protocols.

To address the security requirements for industrial process control systems and components, NIST formed the Process Control Security Requirements Forum (PCSRF) http://www.isd.mel.nist.gov/projects/processcontrol/ in the spring of 2001. The NIST led PCSRF is a working group of users, vendors, and integrators in the process control industry which is addressing the cyber security requirements for industrial process control systems and components, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). Members of the PCSRF represent the critical infrastructures and related process industries, including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 500 members in the PCSRF from government, academic and private sectors, including ABB, Emerson Process Management, Honeywell, Invensys, Rockwell, Cisco, Microsoft, Sun Microsystems, American Gas Association, BP, Chevron Texaco, Exxon Mobile, Association of Metropolitan Water Agencies, American Chemistry Council, Dow, Dupont, Eastman Kodak, Schering-Plough, Georgia-Pacific, I-4, ISA, National Defense University, Idaho National Engineering & Environmental Lab, Pacific Northwest National Lab, Sandia National Lab, Department of Homeland Security, National Security Agency and NIST.

The main goal of the PCSRF is to increase the security of industrial process control systems through the definition and application of a common set of information security requirements for these systems. This will reduce the likelihood of successful cyber-attack on the nation's critical infrastructures. One example of what PCSRF is trying to protect is the operator interface for the control system. The data that is displayed on the operator interface could be coming from sensors and devices many miles away. If this data became compromised, what the operator sees on the screen may not reflect what is really happening. This may cause the operator to take an action, such as flipping a breaker when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required. This could cause loss of production, generation or distribution. The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, is being used to document the results of this effort in the form of Protection Profile security specifications.

The PCSRF System Protection Profile for Industrial Control Systems (SPP-ICS) http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc is designed to present a cohesive, cross-industry, baseline set of security requirements for new industrial control systems. The security requirements specified in the SPP-ICS have been captured from approximately 10 face-to-face meetings of the PCSRF group and specific industry sectors as well as an additional 10 or so conference calls with the group over the past 3 years. The SPP-ICS is designed to be an industry voice to the industrial control system vendors and system integrators, defining the security capabilities that are desired in new products and systems. It is a consensus-based specification, not a NIST specification. These security requirements could be specified in procurement RFPs for new industrial control systems. There is no intent to suggest or imply that the Government will enforce the adaptation of these requirements. The SPP-ICS considers an entire system and addresses requirements for the entire system lifecycle. The SPP-ICS also acts as a starting point for more specific system protection profiles (SCADA, DCS, etc.), for a specific instance of an industrial control system (water, oil/gas, etc.), and for component protection profiles (industrial controller authentication, sensor authentication, etc).

NIST has also initiated the development of a testbed consisting of several implementations of typical industrial control systems including SCADA, networking equipment, as well as relevant sensors and actuators. This Industrial Control System Security Testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines. DOE is working to establish the NIST ICS Security Testbed as an integral part of the National SCADA Testbed with NIST providing expertise in standards and performance metrics.