NSTB Summarizes Vulnerable Areas Commonly Found in Energy Control Systems

Experts at the National SCADA Test Bed (NSTB) discovered some common areas of vulnerability in the energy control systems assessed between late 2004 and early 2006. These vulnerabilities ranged from conventional IT security issues to specific weaknesses in control system protocols. The paper **"Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems"** describes the vulnerabilities and recommended strategies for mitigating them. It should be of use to asset owners and operators, control system vendors, system integrators, and third-party vendors interested in enhancing the security characteristics of current and future products.

In voluntary partnership with forward-thinking vendors, Idaho National Laboratory (INL) has conducted rigorous security assessments of digital control systems to identify vulnerabilities that could put energy systems at risk for a cyber attack. The paper summarizes some of the vulnerability findings common among ten systems assessed under the auspices of the Department of Energy's NSTB Program or the Department of Homeland Security's Control System Security Program, which is managed by INL for the DHS National Cyber Security Division. These systems ranged in complexity from a perimeter protection device, to small digital control systems, to large Supervisory Control and Data Acquisition/Energy Management Systems (SCADA/EMS) with complex networks, multiple servers, and millions of lines of code. The assessments were performed in the INL SCADA Test Bed, in an INL process control systems test bed, and in operational installations (examining non-production or off-line systems).

A more comprehensive report that will include greater detail and the findings from additional assessments is currently under development, but this preliminary paper was released in the interest of moving useful information to industry. Asset owners can use these observations, and the corresponding recommendations for mitigation, to enhance the security of their control systems.