USACM
U.S. Public Policy Committee of the ACM

March 15, 2005

Mr. Carl Paperiello
Director
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington D.C. 20555

Dear Mr. Paperiello:

As chair, I write on behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) to comment on the draft regulatory guide, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants* (DG-1130).

Cybersecurity experts often cite the importance of supervisory control and data acquisition (SCADA) systems and other computer-mediated and controlled systems.[1] Exploitation of vulnerabilities in these systems could have catastrophic effects. Threats to such systems come not only from individuals bent on terrorism or other mischief, but also from subtler sources such as lack of secure design, programming and implementation errors, and human factor issues. For example, in January of 2003 the "slammer" worm infected part of the Davis-Besse nuclear plant's network and shut down a safety system. While this was not a core control system, the event demonstrated that cybersecurity threats to nuclear power plant systems are no longer purely theoretical. I also note that *The Washington Post* recently reported[2] the Federal Energy Regulatory Commissioner's call for stronger cybersecurity in our nation's energy infrastructure. The article specifically points out the potential vulnerabilities of SCADA systems.

In seeking to update the almost decade-old guidance you recognize that protecting computer systems is a crucial component of securing our nation's critical infrastructure. Taking proactive, standards-based steps toward securing computer systems is a necessary and worthwhile process – one long advocated by cybersecurity experts and USACM.

---

[1] See, for example, Chapters 5 and 6 in the National Academies' 2002 report *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, available online at http://www.nap.edu/catalog/10415.html, as well as a forthcoming cybersecurity report from the President's Information Technology Advisory Committee (PITAC), information about which is available at http://www.itrd.gov/pitac/meetings/2005/20050112/20050112_leighton.pdf.

[2] Blum, Justin. "Hackers Target U.S. Power Grid." *The Washington Post* 11 March 2005: E01

As you further develop this voluntary guidance, we encourage you to look toward making these practices mandatory wherever appropriate. It is critical that we establish a stronger security framework for computer systems used in our nation's energy infrastructure – especially in our nation's nuclear power plants. Voluntary guidance should improve the security of these systems, but mandating appropriate cybersecurity requirements is prudent given the potential risks from attack on a nuclear plant's computer systems.

I also wish to offer you the technical and policy expertise of our committee. USACM is the U.S. Public Policy Committee of the Association for Computing Machinery, which is the world's first educational and scientific computing society with almost 80,000 members worldwide. ACM members include leading computer scientists, engineers and other professionals from industry, academia, and government. USACM's mission is to provide non-partisan scientific data, educational materials, and technical analysis to policymakers. Please contact the ACM's Office of Public Policy at (202) 659-9711 if we can provide any assistance on this or related issues.

Sincerely,

Eugene H. Spafford, Ph.D.
Chair
U.S. Public Policy Committee of ACM (USACM)