

**STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
SCADA SYSTEMS AND OUR CRITICAL
INFRASTRUCTURE**

OCTOBER 1, 2003

Thank you Mr. Chairman for calling this hearing, and I thank the witnesses for taking the time to share their experience and expertise with us today.

The vulnerability of the supply of electricity has never been more dramatically demonstrated than the East Coast blackout a few months ago. Just last week nearly all of Italy lost electricity, and similar failures occurred in England and the Netherlands just this summer. The causes of these failures have not been explained to the public. That is troublesome. It is just this kind of vacuum of information in which rumors of conspiracy begin. Are these failures the result of terrorists? Are the systems so inherently complex that even the managers of those systems can't predict their behavior?

There is a more general problem with SCADA systems before us today that is, unfortunately, a familiar one. Computer systems, which are now an integral part of SCADA systems, are vulnerable to worms, viruses, and attacks by hackers and terrorists.

The solution to this problem is not much different than the solutions we have discussed in assuring the protection of government computers -- good management, disciplined

employees, and a recognition that security is the responsibility of everyone in the organization, not just those with security in their title.

The problem of security of SCADA systems is made worse by the introduction of wireless systems. Most government agencies have been reluctant to adopt wireless technology because the ability to secure those systems is not as fully understood. Corporations, on the other hand, have adopted wireless technology extensively in SCADA systems and in corporate management systems. One only has to look at the cost comparisons between hard-wired and wireless systems to understand that move.

We now must make sure that the security of wireless systems catches up to the extensive use of these systems. Today, people routinely walk around the city with wireless computers until they find an open network. They then use that company's wireless network to access the Internet.

I hope our witnesses today will assure the Subcommittee that SCADA systems are not so easily penetrated, and will explain to the Subcommittee the causes of the numerous failures we have experienced.

Thank you Mr. Chairman, and I look forward to today's testimony.