

TOM DAVIS, VIRGINIA,  
CHAIRMAN

DAN BURTON, INDIANA  
CHRISTOPHER SHAYS, CONNECTICUT  
ILEANA ROS-LEHTINEN, FLORIDA  
JOHN M. McHUGH, NEW YORK  
JOHN L. MICA, FLORIDA  
MARK E. SOUDER, INDIANA  
STEVEN C. LATOURETTE, OHIO  
DOUG OSE, CALIFORNIA  
RON LEWIS, KENTUCKY  
JO ANN DAVIS, VIRGINIA  
TODD RUSSELL PLATTIS, PENNSYLVANIA  
CHRIS CANNON, UTAH  
ADAM H. PUTNAM, FLORIDA  
EDWARD L. SCHROCK, VIRGINIA  
JOHN J. DUNCAN, JR., TENNESSEE  
JOHN SULLIVAN, OKLAHOMA  
NATHAN DEAL, GEORGIA  
CANDICE MILLER, MICHIGAN  
TIM MURPHY, PENNSYLVANIA  
MICHAEL R. TURNER, OHIO  
JOHN R. CARTER, TEXAS  
WILLIAM J. JANKLOW, SOUTH DAKOTA  
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

# Congress of the United States

## House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
FACSIMILE (202) 225-3974  
MINORITY (202) 225-5051  
TTY (202) 225-6852

[www.house.gov/reform](http://www.house.gov/reform)

HENRY A. WAXMAN, CALIFORNIA,  
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA  
MAJOR R. OWENS, NEW YORK  
EDOLPHUS TOWNS, NEW YORK  
PAUL E. KANJORSKI, PENNSYLVANIA  
CAROLYN B. MALONEY, NEW YORK  
ELIJAH E. CUMMINGS, MARYLAND  
DENNIS J. KUCINICH, OHIO  
DANNY K. DAVIS, ILLINOIS  
JOHN F. TIERNEY, MASSACHUSETTS  
WM. LACY CLAY, MISSOURI  
DIANE E. WATSON, CALIFORNIA  
STEPHEN F. LYNCH, MASSACHUSETTS  
CHRIS VAN HOLLEN, MARYLAND  
LINDA T. SANCHEZ, CALIFORNIA  
C.A. DUTCH RUPPERSBERGER,  
MARYLAND  
ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA  
JIM COOPER, TENNESSEE  
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,  
INDEPENDENT

## *“The Security of Industrial Control Systems in Our Nation’s Critical Infrastructure.”*

**Wednesday, October 1, 2003  
1:00 p.m.**

*Room 2247 Rayburn House Office Building*

### **Opening Statement of Chairman Adam Putman (R-FI)**

I want to welcome you all today to this hearing on “The Security of Industrial Control Systems in Our Nation’s Critical Infrastructure.” This is the 3<sup>rd</sup> in a series of cyber security hearings that the Subcommittee has conducted over the last couple of weeks, and the 5<sup>th</sup> hearing on this topic since April.

Clearly the issue of protecting the cyber element of our nation’s critical infrastructure is of paramount concern to the Subcommittee and we will continue to examine these matters in a comprehensive manner.

The topic we are discussing today is probably one of the most important we, in our oversight function, can consider. Industrial control systems, often referred to as SCADA, which is an acronym for Supervisory Control and Data Acquisition, underlie most of the infrastructure that makes everyday life possible in the United States.

These systems support the processes that manage our water supply and treatment plants; SCADA systems control the pipeline distribution system and the electric power grid; they operate nuclear and chemical power plants; and they support the manufacturing of food and medicines...just to name a few.

The nation’s health, wealth, and security rely on these systems, but, until recently, computer security for these systems has not been a major focus. As a result, these

systems on which we rely so heavily are undeniably vulnerable to cyber attack or terrorism.

When I first began to learn about this topic, I must say that I did not really grasp the scope of the challenge. Now, the more I know, the more concerned I become. The critical infrastructure of our nation lies mostly in private hands and this nation is dependent on their assessment of risk and economic benefit.

It is also apparent to me that we have not developed a comprehensive strategy for addressing this weakness in our critical infrastructure. As a farmer, I rely on SCADA systems in local dams to prevent my fields from flooding and putting me out of business.

It had never occurred to me that the potential threat from a computer might exceed the harm that could be perpetrated by Mother Nature. I have learned that today's SCADA systems have been designed with little or no attention to computer security.

Data are often sent as clear text; protocols for accepting commands are open, with no authentication required; and communications channels are often wireless, leased lines, or the Internet itself. Remote access into these systems for vendors and maintenance is common. In addition, information about SCADA systems is widely available.

Not only are they increasingly based on common operating systems with well-known vulnerabilities, but information about their vulnerabilities has been widely posted on the World Wide Web.

Finally, SCADA systems now also seem to be victims of common Internet dangers. It has been reported that the blackout this summer may have been partially due to the widespread Blaster worm which apparently disrupted communications among data centers controlling the grid.

The Nuclear Regulatory Agency has recently warned nuclear power plants about infiltration by the Slammer worm after a nuclear plant's systems were infected by a contractor's laptop.

According to U.S. law enforcement and intelligence agencies, SCADA systems, specifically water supply and wastewater management systems, have been the targets of probing by Al Qaeda terrorists.

Some government experts have concluded that terrorists have existing plans to use the Internet as an instrument of bloodshed, by attacking the juncture of cyber systems and the physical systems they control.

A recent National Research Council report has identified "the potential for attack on control systems" as requiring "urgent attention."

Today, we will hear from experts on SCADA design and security, the Federal agencies that oversee them, and from the electricity and oil and gas pipelines sectors. I am hoping to hear something to put my mind at ease, but I am not optimistic.

Finally, I would like to remind everyone that this hearing is being held in executive session. The Subcommittee made that decision for two reasons. The first is that we did not want to provide any information to anyone with malicious intent.

Secondly, I hope that the witnesses will take advantage of this executive session to be candid with the Subcommittee about the extent of the challenges and their concerns, both about current conditions...and prospects for progress in addressing this serious matter.