

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

## *"Telecommunications and SCADA: Secure Links or Open Portals into the Security of the Nation's Critical Infrastructure."*

**Tuesday, March 30, 2004**  
**2:00 p.m.**

*Room 2154 Rayburn House Office Building*

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

I want to welcome you all today to this hearing on "Telecommunications and SCADA: Secure Links or Open Portals into the Security of the Nation's Critical Infrastructure."

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 comprehensively.

This is our second hearing dealing with the issue of SCADA or industrial control systems. Our first hearing was held in a closed session. Through our hearings and other high level briefings, it has become abundantly clear that our Nation is not sufficiently protected from cyber attack against our critical infrastructure. Given the fact that roughly 80% of these systems are owned or controlled by the private sector, it is important that we work collaboratively...and aggressively...to address this serious matter. The testimony today will, obviously, not reveal specific vulnerabilities, however, I hope it will raise the alarm so that the necessary steps will be taken to secure our critical infrastructure from the potential of a cyber attack. Additionally, this hearing will focus attention on the telecommunications that connect SCADA devices to their control and monitoring networks, and review the associated vulnerabilities.

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 America.

These systems support the processes that manage our water supply and treatment plants; control the pipeline distribution system and the electric power grid; operate nuclear and chemical power plants; and 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 have become. The critical infrastructure of our nation lies mostly in private hands and this nation is dependent on their assessment of risk and profit. Many private sector firms are not convinced of the "business case" to invest their resources in information security upgrades. Clearly, there is a much wider acknowledgement of potential physical threats at this point, however, make no mistake...the cyber threat is real...it is 24 x 7...it could come from anywhere...and we must take this threat just as seriously...NOW!

In a book just published, Thomas Reed, a former Air Force Secretary, details how our government allowed the Soviets to steal software used to run gas pipelines. What the Soviets did not know is that the U.S. had sabotaged the software to cause explosions in a Siberian natural gas line.

I became so concerned about the security of our SCADA systems, that I asked the General Accounting Office to report to the Congress on the state of SCADA in America. GAO has produced an outstanding product and we are releasing the report at today's hearing.

Months ago, at the our first SCADA hearing, I said, "It is also apparent to me that we have not developed a comprehensive strategy for addressing this weakness in our critical infrastructure."

In today's GAO report they conclude:

"We are recommending that the Secretary of DHS develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including developing an approach for coordinating the various ongoing efforts to secure control systems. This strategy should also be addressed in the comprehensive national infrastructure plan that the department is tasked to complete by December 2004."

I am looking forward to GAO's testimony as they provide more detail on their findings. 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 also information about their vulnerabilities has been widely posted on the World Wide Web.

Contributing to the security challenge is the requirement for public disclosure about the use of public airwaves. Utilities, factories and power plants must register the frequencies that they use and provide detailed information on the location and structure of their communications networks. Sensitive information about these critical infrastructure systems is easily available. This is a special concern for communications systems that are easily interfered with, such as wireless.

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 warned nuclear power plants about infiltration by the worms and viruses 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."

America must not be so focused on preventing physical attacks that we leave our cyber backdoor wide open and unattended. The tragedy of 9/11 has taught us that we must imagine the unimaginable, prepare for the unthinkable and not leave any stone unturned. To do so could mean devastating economic losses and tragic loss of life. The threat is real and the time to act has long since past.

I look forward to the testimony from today's witnesses and I thank you for your contribution to the security of our Nation.