AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TELECOMMUNICATIONS AND SCADA: SECURE LINKS OR OPEN PORTALS TO THE SECURITY OF OUR NATION'S CRITICAL INFRASTRUCTURE?

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 30, 2004

Serial No. 108–196

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

95–799 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

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 PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
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
——— ———

———

BERNARD SANDERS, Vermont (Independent)

Melissa Wojciak, *Staff Director*
David Marin, *Deputy Staff Director/Communications Director*
Rob Borden, *Parliamentarian*
Teresa Austin, *Chief Clerk*
Phil Barnett, *Minority Chief of Staff/Chief Counsel*

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
——— ———

Ex Officio

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

Bob Dix, *Staff Director*
Dan Daly, *Professional Staff Member*
Juliana French, *Clerk*
Adam Bordes, *Minority Professional Staff Member*

CONTENTS

TELECOMMUNICATIONS AND SCADA: SECURE LINKS OR OPEN PORTALS TO THE SECURITY OF OUR NATION'S CRITICAL INFRASTRUCTURE?

TUESDAY, MARCH 30, 2004

House of Representatives,
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census,
Committee on Government Reform,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:05 p.m., in room 2154, Rayburn House Office Building, Hon. Adam H. Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Miller, and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Dan Daly, professional staff member and deputy counsel; Juliana French, clerk; Suzanne Lightman, fellow; Erik Glavich, legislative assistant; David McMillen and Adam Bordes, minority professional staff members; and Cecelia Morton, minority office manager.

Mr. Putnam. Good afternoon. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

I want to thank everyone for joining us for another important hearing on cyber security. I want to welcome all of you to this hearing entitled, "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 this 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 a closed hearing. Through our hearings and other high level briefings, it has become abundantly clear that our Nation is not protected sufficiently from cyber attack against our critical infrastructure. Given the fact that roughly 80 percent of these systems are owned or controlled by the private sector, it is important that we work collaboratively and aggressively to address this matter. The testimony today will, obviously, not reveal specific vulnerabilities; but I hope it will raise the alarm so that necessary steps will be taken to secure our critical infrastructure from the potential of 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 was not 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 inquire about this topic, I must say that I did not necessarily grasp the scope of the challenge. The more I have learned, the more concerned I have become. The critical infrastructure of our Nation lies mostly in private hands and this Nation is dependent upon their assessment of risk and, certainly, 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. But 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.

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 United States 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 have 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 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 look forward to today's GAO 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 somewhere half way around the world 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 is 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.

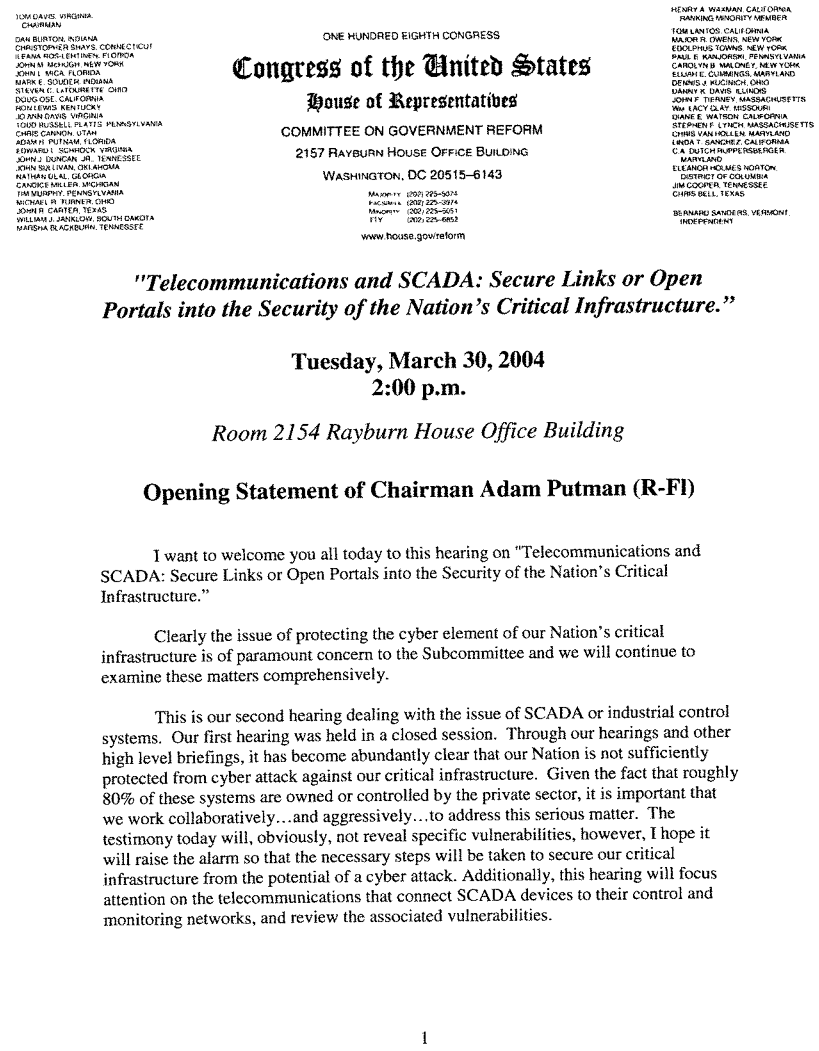
Finally, SCADA systems now also seem to be victims of common Internet dangers. It has been reported that the blackout this summer may have been partially exacerbated due to the widespread Blaster worm, which disrupted communications among data centers controlling the grid. The Nuclear Regulatory Agency 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 back door wide open and unattended. The tragedy of September 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 passed.

I look forward to the testimony from today's witnesses and I thank you for your contribution to the security of our Nation. Today's hearing can be viewed live via Web cast by going to Reform.House.Gov and clicking on the link under "Live Committee Broadcast."

[The prepared statement of Hon. Adam. H. Putnam follows:]



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 PLATTS, 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

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-Fl)

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.

Mr. PUTNAM. I want to welcome the distinguished ranking member of the subcommittee from Missouri, Mr. Clay, and recognize him for his opening statement. You are recognized.

Mr. CLAY. Thank you, Mr. Chairman, especially for calling this hearing. I thank the witnesses for taking the time to share their thoughts with us on how we can best prepare to secure our Nation's critical infrastructure systems.

As all of us remember, the electricity blackout on the East Coast during August 2003 was another warning sign of the trouble which lies ahead should we continue to fail in securing the control networks that deliver us the necessary services for our daily activity. Although the Federal Government has made considerable efforts in producing public-private partnerships to improve the cyber security of our critical infrastructure control systems, a tremendous amount of work remains in coordinating these efforts among Government agencies, private entities, and standard-setting bodies.

Furthermore, if we fail to establish an enforceable public policy blueprint for adequate critical infrastructure protection, how can we expect the necessary implementation of minimal security requirements for control systems throughout the private sector.

Like our hearing last Fall, today's testimony from GAO will detail several challenges inherent in security both public and private control systems against cyber threats from both foreign and domestic sources. They include: our limited technological capacities in securing such systems, the economic cost in providing such security, and indecision within many organizations about making control systems security a priority. These problems are exacerbated by the introduction of new technologies that are not always accompanied by adequate security measures, such as wireless systems. While being both economically and operationally efficient, many technology professionals still lack a detailed understanding of the vulnerabilities contained in wireless systems.

As the subcommittee seeks to define the most practical public policy remedies for these problems, we must be aware of all such variables in order to find an appropriate balance for both governmental and nongovernmental organizations.

As I stated during our hearing on SCADA systems last Fall, "The solution to cyber security and control systems is similar to efforts for resolving security issues in Government computers. The efforts require sound management, skilled and committed employees, and the understanding that security involves all employees in an organization, not just the chief information officer or other designated security officials."

I hope our witnesses today can provide some further insights on how our work should proceed in defining an adequate public policy response in this area. Thank you, Mr. Chairman. I ask that my written testimony be submitted for the record.

Mr. PUTNAM. Without objection.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

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

MARCH 30, 2004

Thank you Mr. Chairman for calling this hearing, and I thank the witnesses for taking the time to share their thoughts with us on how we can best prepare to secure our nation's critical infrastructure systems.

As all of us remember, the electricity blackout on the East Coast during August 2003 was another warning sign of the trouble which lies ahead should we continue to fail in securing the control networks that deliver us the necessary services for our daily activities. Although the federal government has made considerable efforts in producing public-private partnerships to improve the cyber security of our critical infrastructure control systems, a tremendous amount of work remains in coordinating these efforts among government agencies, private entities, and standard-setting bodies.

Furthermore, if we fail to establish an enforceable public policy blueprint for adequate critical infrastructure protection, how can we expect the necessary implementation of minimal security requirements for control systems throughout the private sector?

Like our hearing last fall, today's testimony from GAO will detail several challenges inherent in securing both public and private control systems against cyber threats from both foreign and domestic sources. They include our limited technological capacities in securing such systems, the economic costs in providing such security, and indecision within many organizations about making control system security a priority. These problems are exacerbated by the introduction of new technologies that are not always accompanied by adequate security measures, such as wireless systems. While being both economically and operationally efficient, many technology professionals still lack a detailed understanding of the vulnerabilities contained in wireless systems. As the Subcommittee seeks to define the most practical public policy remedies for these problems, we must be aware of all such variables in order to find an appropriate balance for both governmental and non-governmental organizations.

As I stated during our hearing on SCADA systems last fall, the solution to cyber security in control systems is similar to efforts for resolving security issues in government computers. These efforts require sound management, skilled and committed employees, and the understanding that security involves all employees in an organization, not just the Chief Information Officer or other designated security official.

I hope our witnesses today can provide some further insights on how our work should proceed in defining an adequate public policy response in this area. Thank you Mr. Chairman, and I ask that my written statement be submitted for the record.

Mr. PUTNAM. Thank you, Mr. Clay.

The distinguished vice chair of the subcommittee, the gentlelady from Michigan is also joining us. You are recognized for your opening statement, Mrs. Miller.

Mrs. MILLER. Thank you, Mr. Chairman. I appreciate your holding this very important hearing today. I think as we examine the security of our Nation's critical infrastructure, we certainly are reminded, unfortunately, of our vulnerabilities and the importance of securing our Nation's control systems.

These systems were developed when fears of cyber attacks were non-existent. Certainly their structure and the lack of expansive cyber security frameworks typifies the attitude of our Nation, quite frankly, pre-September 11th when we thought our Homeland was safe from the act of terrorists. But in today's world, the United States is particularly vulnerable because the terrorists look to use our freedoms against us. They look to disrupt our electrical networks, our financial systems, clearly our way of life. These are the things that we tend to take for granted. But we have to be proactive so that we can prevent future attacks from happening.

So the question is, obviously, how can we secure these systems to the best of our ability. And I am hopeful that the witnesses who are testifying today can inform us of how Federal agencies are working with one another, how they are working with the private sector to provide a reasonable solution to the problems that we face. Obviously, building a fail-safe system is impossible but we must strive for what is reasonable. Time is of the essence because an attack on our critical infrastructure can happen from anywhere in the world, at any time. Security of control systems must be given the highest priority, and new technology must continue to be developed.

I certainly want to thank all the witnesses for testifying here today. I am looking forward to your testimony. Thank you, Mr. Chairman.

[The prepared statement of Hon. Candice S. Miller follows:]

Congresswoman Candice S. Miller
GOVERNMENT REFORM COMMITTEE
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
"Telecommunications and SCADA: Secure Links or Open Portals to the Security of Our Nation's Critical Infrastructure"
Tuesday, March 30, 2004

Opening Statement

Mr. Chairman, thank you for holding this very important hearing today. As we examine the security of our nation's critical infrastructure, we are reminded of our vulnerability and the importance of securing our nation's control systems.

These systems were developed when fears of cyber-attacks were non-existent. Their structure, and the lack of expansive cyber-security frameworks, typifies the attitude of a pre-September 11th America – where we thought our homeland was safe from the acts of terrorists. But in today's world, the United

States is particularly vulnerable because the terrorists look to use our freedoms against us. They look to disrupt our electrical networks, our financial systems, and our way of life. These are things we tend to take for granted. But we must be pro-active so that we can prevent future attacks from happening.

The 64 thousand dollar question is how do we secure these systems. I hope the witnesses who are testifying today can inform us how Federal agencies are working with one another – and with the private sector – to provide a collaborative solution to the problems we face.

Time is of the essence because an attack on our critical infrastructure can happen from anywhere in the world and at anytime. Security of control systems must be given the highest priority, and new technology must be developed. We can not wait for a successful attack before we take this threat seriously.

I would like to thank all of the witnesses. I look forward to your testimony.

Thank you.

Mr. PUTNAM. Thank you, Mrs. Miller.

I want to welcome our witnesses again. Mr. Dacey is a frequent flier to the committee. We gave Karen Evans the week off but brought Mr. Dacey back. And as experienced witnesses, you understand the light system so I will not rebrief you on that. As you know, the subcommittee swears in witnesses, and in addition to the seated witnesses, anyone who is joining you who will be contributing to your testimony before the subcommittee.

[Witnesses sworn.]

Mr. PUTNAM. I would note for the record that the witnesses responded in the affirmative.

We will move directly into testimony. Our first witness is Mr. Dacey. Mr. Dacey is currently Director of Information Security Issues at the U.S. General Accounting Office. His responsibilities include evaluating information systems security in Federal agencies and corporations, assessing the Federal infrastructure for managing information security, evaluating the Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats, and identifying best security practices at leading organizations and promoting their adoption by Federal agencies.

You are recognized for 5 minutes. Welcome to the subcommittee. You may proceed.

STATEMENTS OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE; AND JAMES F. MCDONNELL, DIRECTOR, PROTECTIVE SECURITY DIVISION, DEPARTMENT OF HOMELAND SECURITY

Mr. DACEY. Mr. Chairman and members of the subcommittee, I am pleased to be here today to participate in the subcommittee's hearing on the security of control systems. As you requested, I will briefly summarize my written statement which is based on our report on control systems that you released today.

For several years, security risks have been reported in control systems upon which many of the Nation's critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of risks that are specific to control systems, including the adoption of standardized technologies with known vulnerabilities, connectivity of control systems with other networks, insecure remote communications, and widespread availability of technical information about control systems.

Control systems can be vulnerable to a variety of attacks. These attacks could have devastating consequences—such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution by public utilities. Control systems have already been subject to a number of cyber attacks, including documented attacks on a sewage treatment system in Australia in 2000 and, more recently, on a nuclear power plant in Ohio.

Several challenges must be addressed to effectively secure control systems, including one, the lack of specialized security technologies for such systems; two, the perception that securing control systems may not be economically justifiable; and three, conflicting priorities within organizations regarding the security of control systems.

The Department of Homeland Security, other Government agencies, and the private industry have independently initiated several efforts intended to improve the security of control systems. These initiatives include efforts to promote research and development activities, to develop requirements and standards for control systems security, to increase security awareness and information sharing, and to implement effective security management programs. Our report describes these initiatives in greater detail.

Further, implementation of our recommendation for the Department of Homeland Security to develop and implement a strategy to improve control system security, including better coordination of these initiatives, can accelerate progress in securing these critical systems. The department concurred with our recommendation and reported that improving the security of control systems against cyber attack is a high priority for the department.

Additionally, improvements in implementing existing IT technologies and approaches, such as those discussed in our recent report to the subcommittee on commercially available cyber technologies, can accelerate progress in securing these critical systems, including implementing more secure architectures with layered security, for example, by segmenting process control networks with robust firewalls and strong authentication; (2) establishing effective security management programs that include appropriate consideration of control systems; and (3) developing and testing continuity plans within organizations and industries to ensure safe and continued operation in the event of an interruption such as a power outage or a cyber attack, including consideration of interdependencies on other sectors.

In summary, in the face of increasing cyber risks and significant challenges in securing control systems, several initiatives are in progress to improve cyber security of these systems. However, further efforts are needed to address these challenges to carry out and better coordinate such initiatives and to improve implementation of existing technologies and approaches.

Mr. Chairman and members of the subcommittee, this concludes my statement. I would be pleased to answer any questions that you have.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 2 p.m. EST
Tuesday, March 30, 2004

CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

Statement of Robert F. Dacey,
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-04-628T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

March 30, 2004

CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

Why GAO Did This Study

Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines. In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. At the request of the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, this testimony will discuss GAO's March 2004 report on potential cyber vulnerabilities, focusing on (1) significant cybersecurity risks associated with control systems (2) potential and reported cyber attacks against these systems (3) key challenges to securing control systems, and (4) efforts to strengthen the cybersecurity of control systems.

What GAO Recommends

In a March 2004 report, GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with GAO's recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-04-628T.

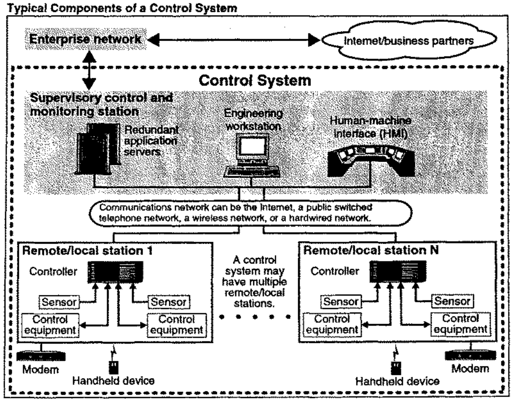
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems. Typical control system components are illustrated in the graphic below. Control systems can be vulnerable to a variety of attacks, examples of which have already occurred. Successful attacks on control systems could have devastating consequences, such as endangering public health and safety.

Securing control systems poses significant challenges, including limited specialized security technologies and lack of economic justification. The government, academia, and private industry have initiated efforts to strengthen the cybersecurity of control systems. The President's *National Strategy to Secure Cyberspace* establishes a role for DHS to coordinate with these entities to improve the cybersecurity of control systems. While some coordination is occurring, DHS's coordination of these efforts could accelerate the development and implementation of more secure systems. Without effective coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

Typical Components of a Control System


Enterprise network
Internet/business partners
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
Controller
Sensor
Sensor
Control equipment
Control equipment
A control system may have multiple remote/local stations.
Remote/local station N
Controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
Handheld device
Modem

Source: GAO (analysis), Art Explosion (clipart).

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to participate in the Subcommittee's hearing on the cyber vulnerabilities in industrial control systems. Control systems—which include supervisory control and data acquisition (SCADA) systems and distributed control systems[1]—perform vital functions across many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing. In October 1997, the President's Commission on Critical Infrastructure Protection highlighted the risk of cyber attacks as a specific point of vulnerability in our critical infrastructures, stating that "the widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."

In my testimony today I will discuss the results of our recent report, which is being released today.[2] As you requested, this report identifies (1) significant cybersecurity risks associated with control systems, (2) potential and reported cyber attacks against these systems, (3) key challenges to securing control systems, and (4) efforts to strengthen the cybersecurity of control systems.

In preparing our report, we analyzed research studies and reports, as well as prior GAO reports and testimonies on critical infrastructure protection (CIP), information security, and national preparedness, among others. We analyzed documents from and met with private-sector and federal officials who had expertise in control systems and their security. Our work was performed from July 2003 to March 2004 in accordance with generally accepted government auditing standards.

[1] Control systems are computer-based systems that are used by many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. There are two primary types of control systems. Distributed Control Systems (DCS) typically are used within a single processing or generating plant or over a small geographic area. Supervisory Control and Data Acquisition (SCADA) systems typically are used for large, geographically dispersed distribution operations.

[2] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* GAO-04-354 (Washington, D.C.: March 15, 2004).

Results in Brief

For several years, security risks have been reported in the control systems on which many of the nation's critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to a steady increase in general cyber threats, several factors have contributed to the escalation of risks specific to control systems, including the (1) adoption of standardized technologies with known vulnerabilities, (2) connectivity of control systems with other networks, (3) insecure remote connections, and (4) widespread availability of technical information about control systems.

Control systems can be vulnerable to a variety of types of cyber attacks that could have devastating consequences—such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution by public utilities. Control systems have already been subject to a number of cyber attacks, including attacks on a sewage treatment system in Australia in 2000 and, more recently, on a nuclear power plant in Ohio.

Securing control systems poses significant challenges. These include the limitations of current security technologies in securing control systems, the perception that securing control systems may not be economically justifiable, and conflicting priorities within organizations regarding the security of control systems.

Government, academia, and private industry have initiated several efforts that are intended to improve the security of control systems. These initiatives include efforts to promote the research and development of new technologies, the development of requirements and standards, an increased awareness and sharing of information, and the implementation of effective security management programs. The President's *National Strategy to Secure Cyberspace* establishes a role for the Department of Homeland Security (DHS) to coordinate with the private sector and other governments to improve the cybersecurity of control systems. While some coordination is occurring, DHS's coordination of these efforts could accelerate the development and implementation of more secure systems. Without adequate coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

In our March report, we recommend 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. DHS's concurred with our recommendation and agreed that improving the security of control systems against cyberattack is a high priority.

Background

Cyberspace Introduces Risks for Control Systems

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day, and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with an unlimited number of individuals and groups.

However, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution systems, water supplies, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. If they are not properly controlled, the speed and accessibility that create the enormous benefits of the computer age may allow individuals and organizations to eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 1 summarizes the key threats to our nation's infrastructures, as observed by the Federal Bureau of Investigation (FBI).

Table 1: Threats to Critical Infrastructures Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence, can affect the daily lives of Americans across the country.[a]
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa macro virus, the Explore.Zip worm, the CIH (Chernobyl) virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a] Prepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Government officials remain concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[3] In addition, the disgruntled organization insider is a significant threat, because these individuals often have knowledge about the organization and its system that allows them to gain unrestricted access and inflict damage or steal assets without knowing a great deal about computer intrusions. As larger amounts of money and more sensitive economic and commercial information are exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on standardized information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

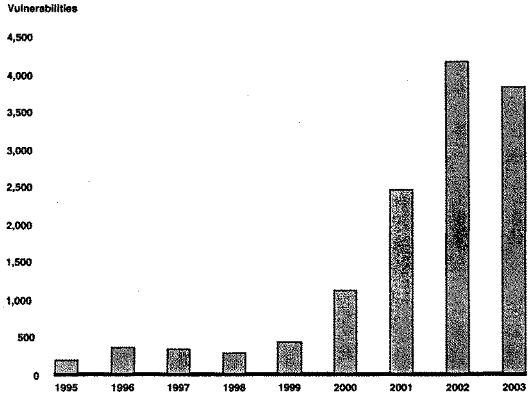
As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can download tools from the Internet and literally "point and click" to start an attack. Experts agree that there has been a steady advance in the level of sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities that have been discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan networks for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

From 1995 through 2003, the CERT® Coordination Center[4] (CERT/CC) reported 12,946 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities over these years. The growing number of known vulnerabilities increases the potential for attacks by the hacker community. Attacks can be launched against specific targets or widely distributed through viruses and worms.

[3] *Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as termination of the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

[4] The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

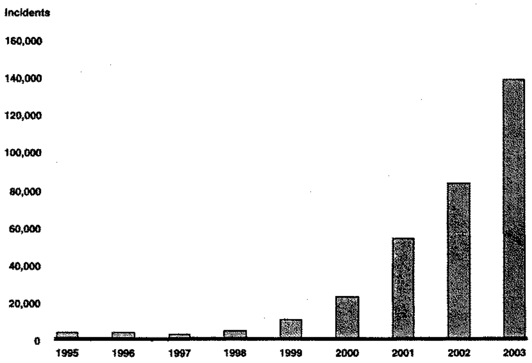
Figure 1: Security Vulnerabilities, 1995–2003



Source: GAO analysis based on Carnegie Mellon University's CERT® Coordination Center data.

Along with these increasing vulnerabilities, the number of computer security incidents reported to CERT/CC has also risen dramatically—from 9,859 in 1999 to 82,094 in 2002 and to 137,529 in 2003. And these are only the reported attacks. The Director of the CERT Centers has estimated that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) there were no indications of penetration or attack, (2) the organization was unable to recognize that its systems had been penetrated, or (3) the organization was reluctant to report. Figure 2 shows the number of incidents that were reported to the CERT/CC from 1995 through 2003.

Figure 2: Computer Security Incidents, 1995–2003



Source: GAO analysis based on Carnegie Mellon University's CERT® Coordination Center data.

According to the National Security Agency (NSA), foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. The National Infrastructure Protection Center (NIPC) reported in January 2002 that a computer belonging to an individual who had indirect links to Osama bin Laden contained computer programs that indicated that the individual was interested in the structural engineering of dams and other water-retaining structures. The NIPC report also stated that U.S. law enforcement and intelligence agencies had received indications that Al Qaeda members had sought information about control systems from multiple Web sites, specifically on water supply and wastewater management practices in the United States and abroad.

Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have increased. For example, in his February 2002 statement for the Senate Select Committee on Intelligence, the Director of Central Intelligence discussed the possibility of a cyber warfare attack by terrorists.[5] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them. James Woolsey, a former Director of Central Intelligence, shares this concern, and on October 29, 2003, in a speech before several hundred security experts, he warned that the nation should be prepared for continued terrorist attacks on our critical infrastructures. Moreover, a group of concerned scientists warned President Bush in a letter that "the critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster." According to a study by a computer security organization, during the second half of 2003, critical infrastructure industries such as power, energy, and financial services experienced high attack rates.[6] Further, a study that surveyed over 170 security professionals and other executives concluded that, across industries, respondents believe that a large-scale cyber attack in the United States will be launched against their industry by mid-2006.

What Are Control Systems?

Control systems are computer-based systems that are used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. In the electric power industry, control systems can manage and control the generation, transmission, and distribution of electric power— for example, by opening and closing circuit breakers and setting thresholds for preventive shutdowns. Employing integrated control systems, the oil and gas industry can control the refining operations at a plant site, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission. Water utilities can

[5] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 6, 2002.

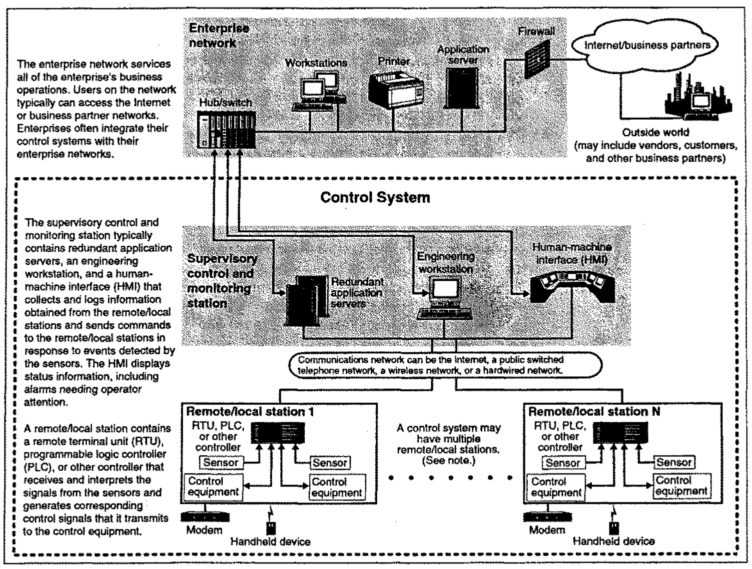
[6] Symantec, *Symantec Internet Security Threat Report: Trends for July 1, 2003-December 31, 2003* (March 2004).

remotely monitor well levels and control the wells' pumps; monitor flows, tank levels, or pressure in storage tanks; monitor water quality characteristics—such as pH, turbidity, and chlorine residual; and control the addition of chemicals. Control systems also are used in manufacturing and chemical processing. Control systems perform functions that vary from simple to complex; they can be used simply to monitor processes—for example, the environmental conditions in a small office building—or to manage most activities in a municipal water system or even a nuclear power plant.

In certain industries, such as chemical and power generation, safety systems are typically implemented in order to mitigate a potentially disastrous event if control and other systems should fail. In addition, to guard against both physical attack and system failure, organizations may establish backup control centers that include uninterruptible power supplies and backup generators.

There are two primary types of control systems. Distributed Control Systems (DCS) typically are used within a single processing or generating plant or over a small geographic area. Supervisory Control and Data Acquisition (SCADA) systems typically are used for large, geographically dispersed distribution operations. For example, a utility company may use a DCS to generate power and a SCADA system to distribute it. Figure 3 illustrates the typical components of a control system.

Figure 3: Typical Components of a Control System



Enterprise network
Workstations
Printer
Application server
Firewall
Internet/business partners
Hub/switch
Outside world
(may include vendors, customers, and other business partners)
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
A control system may have multiple remote/local stations. (See note.)
Remote/local station N
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device

The enterprise network services all of the enterprise's business operations. Users on the network typically can access the Internet or business partner networks. Enterprises often integrate their control systems with their enterprise networks.

The supervisory control and monitoring station typically contains redundant application servers, an engineering workstation, and a human-machine interface (HMI) that collects and logs information obtained from the remote/local stations and sends commands to the remote/local stations in response to events detected by the sensors. The HMI displays status information, including alarms needing operator attention.

A remote/local station contains a remote terminal unit (RTU), programmable logic controller (PLC), or other controller that receives and interprets the signals from the sensors and generates corresponding control signals that it transmits to the control equipment.

Source: GAO (analysis), Art Explosion (clipart).

Note: Remote/local stations can include one or more interfaces to allow field operators to perform diagnostic and maintenance operations. Sensors can measure level, pressure, flow, current, voltages, etc., depending on the infrastructure. Control equipment can be valves, pumps, relays, circuit breakers, etc., also depending on the infrastructure.

A control system typically is made up of a “master” or central supervisory control and monitoring station consisting of one or more human-machine interfaces where an operator can view status information about the remote/local sites and issue commands directly to the system. Typically, this station is located at a main site, along with application servers and an engineering workstation that is used to configure and troubleshoot the other components of the control system. The supervisory control and monitoring station typically is connected to local controller stations through a hard-wired network or to a remote controller station through a communications network—which could be the Internet, a public switched telephone network, or a cable or wireless (e.g., radio, microwave, or Wi-Fi[7]) network. Each controller station has a remote terminal unit (RTU), a programmable logic controller (PLC), or some other controller that communicates with the supervisory control and monitoring station.

The control system also includes sensors and control equipment that connect directly with the working components of the infrastructure—for example, pipelines, water towers, or power lines. The sensor takes readings from the infrastructure equipment—such as water or pressure levels, electrical voltage or current—and sends a message to the controller. The controller may be programmed to determine a course of action and send a message to the control equipment instructing it what to do—for example, to turn off a valve or dispense a chemical. If the controller is not programmed to determine a course of action, the controller communicates with the supervisory control and monitoring station and relays instructions back to the control equipment. The control system also can be programmed to issue alarms to the operator when certain conditions are detected. Handheld devices, such as personal digital assistants, can be used to locally monitor controller stations. Experts report that technologies in controller stations are becoming more intelligent and automated and are able to communicate with the supervisory central monitoring and control station less frequently, thus requiring less human intervention.

Control Systems Are at Increasing Risk

Historically, security concerns about control have been related primarily to protecting them against physical attack and preventing the misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

In October 1997, the President's Commission on Critical Infrastructure Protection discussed the potential damaging effects on the electric power

[7] Wi-Fi (short for wireless fidelity) is the popular term for a high-frequency wireless local area network.

and oil and gas industries of successful attacks on control systems.[8] Moreover, in 2002, the National Research Council identified "the potential for attack on control systems" as requiring "urgent attention."[9] In the first half of that year, security experts reported that 70 percent of energy and power companies experienced at least one severe cyber attack. In February 2003, the President clearly demonstrated concern about "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security," noting that "disruption of these systems can have significant consequences for public health and safety" and emphasizing that the protection of control systems has become "a national priority."[10]

Several factors have contributed to the escalation of risk to control systems, including (1) the adoption of standardized technologies with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems.

Control Systems Are Adopting Standardized Technologies with Known Vulnerabilities

In the past, proprietary hardware, software, and network protocols made it difficult to understand how control systems operated—and therefore how to hack into them. Today, however, to reduce costs and improve performance, organizations have been transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft's Windows, Unix-like operating systems, and the common networking protocols used by the Internet. These widely-used, standardized technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools are widely available and relatively easy to use. As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subject to attack have increased. Also, common communication protocols and the emerging use of extensible markup language (commonly referred to as XML) can make it easier for a hacker to interpret the content of communications among the components of a control system.

[8] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: October 1997).

[9] The National Research Council, Making the Nation Safer: the Role of Science and Technology in Countering Terrorism (Washington, D.C.: December 2002).

[10] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

Control Systems Are Connected to Other Networks

Enterprises often integrate their control systems with their enterprise networks. This increased connectivity has significant advantages, including providing decision makers with access to real-time information and allowing engineers to monitor and control the process control system from different points on the enterprise network. In addition, the enterprise networks are often connected to the networks of strategic partners and to the Internet. Furthermore, control systems are increasingly using wide area networks and the Internet to transmit data to their remote or local stations and individual devices. This convergence of control networks with public and enterprise networks potentially creates further security vulnerabilities in control systems. Unless appropriate security controls are deployed in both the enterprise network and the control system network, breaches in enterprise security can affect the operation of control systems.

Insecure Connections Exacerbate Vulnerabilities

Vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links—such as dial-up modems to equipment and control information—open for remote diagnostics, maintenance, and examination of system status. If such links are not protected with authentication or encryption, the risk increases that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities. Without encryption to protect data as it flows through these insecure connections or authentication mechanisms to limit access, there is little to protect the integrity of the information being transmitted.

Information about Infrastructures and Control Systems Is Publicly Available

Public information about infrastructures and control systems is readily available to potential hackers and intruders. The availability of this infrastructure and vulnerability data was demonstrated last year by a George Mason University graduate student who, in his dissertation, reportedly mapped every business and industrial sector in the American economy to the fiber-optic network that connects them, using material that was available publicly on the Internet—and not classified.

In the electric power industry, open sources of information—such as product data and educational videotapes from engineering associations—can be used to understand the basics of the electrical grid. Other publicly available information—including filings of the Federal Energy Regulatory Commission (FERC), industry publications, maps, and material available on the Internet—is sufficient to allow someone to identify the most heavily loaded transmission lines and the most critical substations in the power grid. Many of the electric utility officials who were interviewed for the National Security Telecommunications Advisory Committee's Information Assurance Task Force's Electric Power Risk Assessment expressed concern over the amount of information about their infrastructure that is readily available to the public.

In addition, significant information on control systems is publicly available—including design and maintenance documents, technical standards for the interconnection of control systems and RTUs, and standards for communication among control devices—all of which could assist hackers in understanding the systems and how to attack them. Moreover, there are numerous former employees, vendors, support contractors, and other end users of the same equipment worldwide who have inside knowledge about the operation of control systems.

Security experts have stated that an individual with very little knowledge of control systems could gain unauthorized access to a control system using a port scanning tool and a factory manual that can be easily found on the Internet and that contains the system's default password. As noted in the following discussion, many times these default passwords are never changed.

Cyber Threats to Control Systems

There is a general consensus—and increasing concern—among government officials and experts on control systems about potential cyber threats to the control systems that govern our critical infrastructures. As components of control systems increasingly make vital decisions that were once made by humans, the potential effect of a cyber attack becomes more devastating. Cyber threats could come from numerous sources ranging from hostile governments and terrorist groups to disgruntled employees and other malicious intruders. Based on interviews and discussions with representatives from throughout the electric power industry, the Information Assurance Task Force of the National Security Telecommunications Advisory Committee concluded that an organization with sufficient resources, such as a foreign intelligence service or a well-supported terrorist group, could conduct a structured attack on the electric power grid electronically, with a high degree of anonymity, and without having to set foot in the target nation.

In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," was an emerging threat to the critical infrastructure of the United States. As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For instance, a cyber attack that disabled the water supply or the electrical system, in conjunction with a physical attack, could deny emergency services the necessary resources to manage the consequences of the physical attack—such as controlling fires, coordinating response, and generating light.

According to the National Institute of Standards and Technology (NIST), cyber attacks on energy production and distribution systems—including electric, oil, gas, and water treatment, as well as on chemical plants containing potentially hazardous substances—could endanger public health and safety, damage the environment, and have serious financial implications such as loss of production, generation, or distribution by public utilities; compromise of proprietary information; or liability issues. When backups for damaged components are not readily available (e.g., extra-high-voltage transformers for the electric power grid), such damage could have a long-lasting effect. I will now discuss potential and reported cyber attacks on control systems, as well as challenges to securing them.

Control Systems Can Be Vulnerable to Cyber Attacks

Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems:

- disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;
- make unauthorized changes to programmed instructions in PLCs, RTUs, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control equipment that could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling control equipment;
- send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;

- modify the control system software, producing unpredictable results; and
- interfere with the operation of safety systems.

In addition, in control systems that cover a wide geographic area, the remote sites often are not staffed and may not be physically monitored. If such remote systems were to be physically breached, attackers could establish a cyber connection to the control network.

Department of Energy (DOE) and industry researchers have speculated on how the following potential attack scenario could affect control systems in the electricity sector. Using war dialers[11] to find modems connected to the programmable circuit breakers of the electric power control system, hackers could crack passwords that control access to the circuit breakers and could change the control settings to cause local power outages and even damage equipment. A hacker could lower settings from, for example, 500 amperes[12] to 200 on some circuit breakers; normal power usage would then activate, or "trip," the circuit breakers, taking those lines out of service and diverting power to neighboring lines. If, at the same time, the hacker raised the settings on these neighboring lines to 900 amperes, circuit breakers would fail to trip at these high settings, and the diverted power would overload the lines and cause significant damage to transformers and other critical equipment. The damaged equipment would require major repairs that could result in lengthy outages.

Control system researchers at DOE's national laboratories have developed systems that demonstrate the feasibility of a cyber attack on a control system at an electric power substation where high-voltage electricity is transformed for local use. Using tools that are readily available on the Internet, they are able to modify output data from field sensors and take control of the PLC directly in order to change settings and create new output. These techniques could enable a hacker to cause an outage, thus incapacitating the substation.

Experts in the water industry consider control systems to be among the primary vulnerabilities of drinking water systems. A technologist from the water distribution sector has demonstrated how an intruder could hack into the communications channel between the control center of a water distribution pump station and its remote units, located at water storage

[11] War dialers are simple personal computer programs that dial consecutive phone numbers looking for modems.

[12] An ampere is a unit of measurement for electric current.

and pumping facilities, to either block messages or send false commands to the remote units. Moreover, experts are concerned that terrorists could, for example, trigger a cyber attack to release harmful amounts of water treatment chemicals, such as chlorine, into the public's drinking water.

Cyber Attacks on Control Systems Have Been Reported

Experts in control systems have verified numerous incidents that have affected control systems. Reported attacks include the following:

- In 1994, the computer system of the Salt River Project, a major water and electricity provider in Phoenix, Arizona, was breached.
- In March 1997, a teenager in Worcester, Massachusetts, remotely disabled part of the public switching network, disrupting telephone service for 600 residents and the fire department and causing a malfunction at the local airport.
- In the spring of 2000, a former employee of an Australian company that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely hack into the controls of a sewage treatment system and ultimately release about 264,000 gallons of raw sewage into nearby rivers and parks.
- In the spring of 2001, hackers mounted an attack on systems that were part of a development network at the California Independent System Operator, a facility that is integral to the movement of electricity throughout the state.
- In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm—otherwise known as Slammer—infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.

In addition, in 1997, the Department of Defense (DOD) undertook the first systematic exercise to determine the nation's and DOD's vulnerability to cyberwar. During a 2-week military exercise known as Eligible Receiver, staff from NSA used widely available tools to show how to penetrate the control systems that are associated with providers of electric power to DOD installations. Other assessments of control systems at DOD installations have demonstrated vulnerabilities and identified risks in the installations' network and operations.

Securing Control Systems Poses Significant Challenges

The control systems community faces several challenges to securing control systems against cyber threats. These challenges include (1) the limitations of current security technologies in securing control systems, (2) the perception that securing control systems may not be economically justifiable, and (3) the conflicting priorities within organizations regarding the security of control systems.

Lack of Specialized Security Technologies for Control Systems

According to industry experts, existing security technologies, as well as strong user authentication and patch management practices, are generally not implemented in control systems because control systems usually have limited processing capabilities, operate in real time, and are typically not designed with cybersecurity in mind.

Existing security technologies[13] such as authorization, authentication, encryption, intrusion detection, and filtering of network traffic and communications, require more bandwidth, processing power, and memory than control system components typically have. Controller stations are generally designed to do specific tasks, and they often use low-cost, resource-constrained microprocessors. In fact, some control system devices still use the Intel 8088 processor, which was introduced in 1978. Consequently, it is difficult to install current security technologies without seriously degrading the performance of the control system.

For example, complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because this could hinder a rapid response to safety procedures during an emergency. As a result, according to experts, weak passwords that are easy to guess, shared, and infrequently changed are reportedly common in control systems, including the use of default passwords or even no password at all.

[13] See U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 9, 2004) for a discussion of cybersecurity technologies.

In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches may be either incompatible with the customized version of the operating system or difficult to implement without compromising service by shutting down "always-on" systems or affecting interdependent operations. Another constraint on deploying patches is that support agreements with control system vendors often require the vendor's approval before the user can install patches. If a patch is installed in violation of the support agreement, the vendor will not take responsibility for potential impacts on the operations of the system. Moreover, because a control system vendor often requires that it be the sole provider of patches, if the vendor delays in providing patches, systems remain vulnerable without recourse.

Information security organizations have noted that a gap exists between currently available security technologies and the need for additional research and development to secure control systems. Research and development in a wide range of areas could lead to more effective technologies. For example, although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from external networks, research and development could help to address the application of security technologies to the control systems themselves. Other areas that have been noted for possible research and development include identifying the types of security technologies needed for different control system applications, determining acceptable performance trade-offs, and recognizing attack patterns for use in intrusion detection systems.

Industry experts have identified challenges in migrating system components to newer technologies while maintaining uninterrupted operations. Upgrading all the components of a control system can be a lengthy process, and the enhanced security features of newly installed technologies—such as their ability to interpret encrypted messages—may not be able to be fully utilized until all devices in the system have been replaced and the upgrade is complete.

Securing Control Systems May Not Be Perceived as Economically Justifiable

Experts and industry representatives have indicated that organizations may be reluctant to spend more money to secure control systems. Hardening the security of control systems would require industries to expend more resources, including acquiring more personnel, providing training for personnel, and potentially prematurely replacing current systems, which typically have a lifespan of about 20 years.

Several vendors suggested that since there have been no reports of significant disruptions caused by cyber attacks on U.S. control systems, industry representatives believe the threat of such an attack is low. While incidents have occurred, to date there is no formalized process for collecting and analyzing information about control systems incidents, thus further contributing to the skepticism of control systems vendors. We have previously recommended that the government work with the private sector to improve the quality and quantity of information being shared among industries and government about attacks on the nation's critical infrastructures.[14]

Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems. We have previously reported that consideration of further federal government efforts is needed to provide appropriate incentives for nonfederal entities to enhance their efforts to implement CIP—including protection of control systems. Without appropriate consideration of public policy tools, such as regulation, grants, and tax incentives, private-sector participation in sector-related CIP efforts may not reach its full potential.[15]

Organizational Priorities Conflict

Finally, several experts and industry representatives indicated that the responsibility for securing control systems typically includes two separate groups: (1) IT security personnel and (2) control system engineers and operators. IT security personnel tend to focus on securing enterprise systems, while control system engineers and operators tend to be more concerned with the reliable performance of their control systems. These experts indicate that, as a result, those two groups do not always fully understand each other's requirements and so may not effectively collaborate to implement secure control systems.

These conflicting priorities may perpetuate a lack of awareness of IT security strategies that could be deployed to mitigate the vulnerabilities of

[14] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

[15] U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sept. 17, 2003).

control systems without affecting their performance. Although research and development will be necessary to develop technologies to secure individual control system devices, existing IT security technologies and approaches could be implemented as part of a secure enterprise architecture to protect the perimeters of, and access to, control system networks. Existing IT security technologies include firewalls, intrusion-detection systems, encryption, authentication, and authorization. Approaches to IT security include segmenting control system networks and testing continuity plans to ensure safe and continued operation.

To reduce the vulnerabilities of its control system, officials from one company formed a team composed of IT staff, process control engineers, and manufacturing employees. This team worked collaboratively to research vulnerabilities and to test fixes and workarounds.

Efforts to Strengthen the Cybersecurity of Control Systems Under Way, but Lack Adequate Coordination

Government, academia, and private industry have independently initiated multiple efforts and programs focused on some of the key areas that should be addressed to strengthen the cybersecurity of control systems. Our March 2004 report includes a detailed discussion of many initiatives. The key areas—and illustrative examples of ongoing efforts in these areas—include the following:

- **Research and development of new security technologies to protect control systems.** Both federal and nonfederal entities have initiated efforts to develop encryption methods for securing communications on control system networks and field devices. Moreover, DOE is planning to establish a National SCADA Test Bed to test control system vulnerabilities. However, funding constraints have delayed the implementation of the initial phases of these plans.
- **Development of requirements and standards for control system security.** Several entities are working to develop standards that increase the security of control systems. The North American Electric Reliability Council (NERC) is preparing to draft a standard that will include security requirements for control systems. In addition, the Process Controls Security Requirements Forum (PCSRF), established by NIST and NSA, is working to define a common set of information security requirements for control systems. However, according to NIST officials, reductions to fiscal year 2004 appropriations will delay these efforts.

- **Increased awareness of security and sharing of information about the implementation of more secure architectures and existing security technologies.** To promote awareness of control system vulnerabilities, DOE has created security programs, trained teams to conduct security reviews, and developed cybersecurity courses. The Instrumentation Systems and Automation Society has reported on the known state of the art of cybersecurity technologies as they are applied to the control systems environment, to clearly define what technologies can currently be deployed.
- **Implementation of effective security management programs, including policies and guidance that consider control system security.** Both federal and nonfederal entities have developed guidance to mitigate the security vulnerabilities of control systems. DOE's *21 Steps to Improve Cyber Security of SCADA Networks* provides guidance for improving the security of control systems and establishing underlying management processes and policies to help organizations improve the security of control system networks.

In previous reports, we have recommended the development of a comprehensive and coordinated national plan to facilitate the federal government's CIP efforts. This plan should clearly delineate the roles and responsibilities of federal and nonfederal CIP entities, define interim objectives and milestones, set time frames for achieving objectives, and establish performance measures.

The President in his homeland security strategies and Congress in enacting the Homeland Security Act designated DHS as responsible for developing a comprehensive national infrastructure plan. The plan is expected to inform DHS on budgeting and planning for CIP activities and on how to use policy instruments to coordinate among government and private entities to raise the security of our national infrastructures to appropriate levels. According to Homeland Security Presidential Directive 7 (HSPD 7), issued December 17, 2003, DHS is to develop this formalized plan by December 2004.

In February 2003, the President's *National Strategy to Secure Cyberspace* established a role for DHS to coordinate with other government agencies and the private sector to improve the cybersecurity of control systems. DHS's assigned role includes:

- ensuring that there is broad awareness of the vulnerabilities in control systems and the consequences of exploiting these vulnerabilities,

- developing best practices and new technologies to strengthen the security of control systems, and
- identifying the nation's most critical control system sites and developing a prioritized plan for ensuring cyber security at those sites.

In addition, the President's strategy recommends that DHS work with the private sector to promote voluntary standards efforts and the creation of security policy for control systems.

DHS recently began to focus on the range of activities that are under way among the numerous entities that are working to address these areas. In October 2003, DHS's Science and Technology Directorate initiated a study to determine the current state of security of control systems. In December 2003, DHS established the Control Systems Section within the Protective Security Division of its Information Analysis and Infrastructure Protection (IAIP) Directorate. The objectives of this section are to identify computer-controlled systems that are vital to infrastructure functions, evaluate the potential threats to these systems, and develop strategies that mitigate the consequences of attacks. In addition, IAIP's National Cyber Security Division (NCSD) is planning to develop a methodology for conducting cyber assessments across all critical infrastructures, including control systems. The objectives of this effort include defining specific goals for the assessments and, based on their results, developing sector-specific recommendations to mitigate vulnerabilities. NCSD also plans to examine processes, technology, and available policy, procedures, and guidance. Because these efforts have only recently been initiated, DHS acknowledges that it has not yet developed a strategy for implementing the functions mentioned above.

As I previously mentioned, many government and nongovernment entities are spearheading various initiatives to address the challenge of implementing cybersecurity for the vital systems that operate our nation's critical infrastructures. While some coordination is occurring, both federal and nonfederal control systems experts have expressed their concern that these efforts are not being adequately coordinated among government agencies, the private sector, and standards-setting bodies. DHS's coordination of these efforts could accelerate the development and implementation of more secure systems to manage our critical infrastructures. In contrast, insufficient coordination could contribute to

- delays in the general acceptance of security requirements and the adoption of successful practices for control systems,

- failure to address gaps in the research and development of technologies to better secure control systems,
- impediments to standards-creating efforts across industries that could lead to less expensive technological solutions, and
- reduced opportunities for efficiency that could be gained by leveraging ongoing work.

In summary, it is clear that the systems that monitor and control the sensitive processes and physical functions of the nation's critical infrastructures are at increasing risk from threats of cyber attacks. Securing these systems poses significant challenges. Numerous federal agencies, critical infrastructure sectors, and standards-creating bodies are leading various initiatives to address these challenges. DHS's implementation of our recommendation—with which the department concurred—to develop and implement a strategy for better coordinating the cybersecurity of our critical infrastructures' control systems among government and private sector entities can accelerate progress in securing these critical systems. Additionally, implementing existing IT technologies and security approaches can strengthen the security of control systems. These approaches include establishing an effective security management program, building successive layers of defense mechanisms at strategic access points to the control system network, and developing and testing continuity plans to ensure safe operation in the event of a power outage or cyber attack.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this statement, please contact me at (202) 512-3317 or Elizabeth Johnston, Assistant Director, at (202) 512-6345. We can also be reached by e-mail at daceyr@gao.gov and johnstone@gao.gov, respectively.

Other individuals who made key contributors to this testimony include Shannin Addison, Joanne Fiorino, Alison Jacobs, Anjalique Lawrence, and Tracy Pierson.

Mr. PUTNAM. Thank you, Mr. Dacey.

Our second witness on our first panel is James McDonnell. Mr. McDonnell is the Director of the Protective Security Division at the Department of Homeland Security. Prior to this position, Mr. McDonnell was the Director of Energy Assurance at the Department of Energy, and director of national security operations at Oak Ridge associate universities. Mr. McDonnell has over 25 years of experience managing national security and homeland security activities and was a member of the leadership team assigned to craft the Department of Homeland Security in the White House Transition Planning Office. In 1995, Mr. McDonnell completed a 20 year career as an officer in special operations and special warfare in the U.S. Navy.

I want to welcome you to the subcommittee. We appreciate the experience that you bring. You are recognized for 5 minutes.

Mr. MCDONNELL. Good afternoon Chairman Putnam and distinguished members of the subcommittee. It is an honor to appear before you today to discuss activities that the Department of Homeland Security is engaged in regarding process control systems and our Nation's critical infrastructure. I am James McDonnell, Director of the Protective Security Division, part of the Information Analysis and Infrastructure Protection Directorate within the Department.

Established by the Homeland Security Act, and directed by Homeland Security Presidential Directives, IAIP is responsible for reducing the Nation's vulnerability to terrorism by one, developing and coordinating plans to protect critical infrastructure and key assets; and two, denying the use of the infrastructure as a weapon.

Our goal is to ensure a national capacity to detect indicators of terrorist activity, deter attacks, and devalue targets, and to defend potential targets against terrorist threats to our critical infrastructures.

To meet this goal, IAIP identifies those sites and facilities that may be an attractive target for terrorists based on risk and identifies how best to reduce those vulnerabilities. Once we know what we should protect and what the vulnerabilities are, we conduct risk assessments. We map threat and vulnerability information. This information is then used to prioritize the implementation of protective measures focused on mitigating our Nation's vulnerability to attack and, more importantly, sharing in a timely manner that information with State and local officials.

The complexity of the infrastructure requires a comprehensive understanding of how this "system of systems" operates and it is this complexity that adds another dimension of vulnerability—the use of complex process control systems.

Process control systems are industrial measurement and control systems used to monitor and control plants and equipment. They are utilized in numerous industries, including energy, manufacturing, chemical production and storage, food processing, and drinking water and water treatment facilities. These systems are often referred to generically by one of the most prevalent types, SCADA, Supervisory Control and Data Acquisition, but there are many other types of these systems.

The systems vary in function, size, complexity, and age. Some function in an automated fashion. Some rely on a human/machine interface, where the system provides critical information upon which an operator bases process control decisions. Some digital controls systems can be reprogrammed from offsite through dial-up connections or through Web-based access. This cyber-physical nexus creates a complexity that requires a comprehensive approach for protection.

To address the protection of these critical systems, IAIP has developed a comprehensive strategy to protect each element of process control systems. Our focus is on joint Government-industry efforts to identify key assets, discover vulnerabilities, analyze risk, implement effective protective measures, conduct joint exercises and training, disseminate information, and develop inherently safer technology. Since most process control systems reside in the private sector, our ability to always effect change is sometimes affected by business factors that we cannot control.

IAIP manages this as a team effort that includes all parts of the Directorate, including the Protective Security Division, the National Cyber Security Division, the Infrastructure Coordination Division, and the National Communication System. The bulk of the remediation and protective activities are conducted by PSD and National Cyber Security Division.

Immediate efforts focus on protective measures that can be implemented within the as installed/legacy environment, such as inexpensive technical or procedural changes that can be implemented at the site and in the immediate future. Near term efforts include detailed testing and assessment of vulnerabilities. In the long term, we will work with the private sector on the development of inherently safer technology.

As part of PSD, we have established a Control Systems Section that will oversee the SCADA security program. The Control Systems Section will identify and reduce vulnerabilities critical to domestic security related to control systems. This section also includes the development and integration of the understanding of offensive capabilities, and providing relevant hands-on operational support during DHS heightened security events.

We have identified approximately 1,700 facilities across the country that we hope to engage in a major vulnerability reduction effort during fiscal year 2004. Of those sites, we have identified 565 with process control systems. As appropriate, reduction in SCADA vulnerabilities will be undertaken just as reductions in physical vulnerabilities are.

In closing, I would like to reiterate first that SCADA vulnerabilities are a fact, just like a hole in a perimeter fence. The problem is that the SCADA vulnerability is not seen by the casual observer and therefore goes easily unnoticed. SCADA vulnerabilities are seen by those who would do us harm through their manipulation and it is incumbent upon IAIP to ensure that those responsible for protecting America are seeing them and doing something about it. Finally, as earlier stated, the Department of Homeland Security views this as a national effort involving many directorates within the Department and many organizations, both public and private, outside DHS.

I would be happy to answer any questions you may have.

[The prepared statement of Mr. McDonnell follows:]

Statement of James F. McDonnell
Director, Protective Security Division,
Information Analysis and Infrastructure Protection Directorate
Department of Homeland Security
Before the
Government Reform Committee's Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
U.S. House of Representatives
March 30, 2004

Good morning Chairman Putnam and distinguished Members of the Subcommittee. It is an honor to appear before you today to discuss activities that the Department of Homeland Security is engaged in regarding process control systems in our Nation's critical infrastructure. I am James McDonnell, Director of the Protective Security Division (PSD), part of the Department's Information Analysis and Infrastructure Protection Directorate (IAIP).

Established by the *Homeland Security Act,* and directed by Homeland Security Presidential Directives, IAIP is responsible for reducing the Nation's vulnerability to terrorism by:

- Developing and coordinating plans to protect critical infrastructure and key assets.
- Denying the use of our infrastructure as a weapon.

Our goal is to ensure a national capacity to detect indicators of terrorist activity, deter attacks, and devalue targets and to defend potential targets against terrorist threats to our critical infrastructure.

To meet this goal, IAIP identifies those sites and facilities that may be attractive targets for terrorists based on risk and identifies how target vulnerabilities may be exploited by terrorists. Once we know what we should protect and what the vulnerabilities are, we conduct risk assessments, mapping threat and vulnerability information. This information is then used to prioritize the implementation of protective measures focused on mitigating our Nation's vulnerability to attack and, more importantly, shared in a timely manner with State and local officials.

Terrorist acts come in many forms. Some result in loss of life, others in severe economic consequences. Some, like September 11, result in both. Terrorist attacks do not have to follow a pattern and may range from a bombing by an individual to a global internet-based cyber attack. Protecting our way of life means understanding the myriad of vulnerabilities and the associated interdependencies and cascading effects.

The complexity of the infrastructure requires a comprehensive understanding of how the "system of systems" operates and it is this complexity that adds another dimension of vulnerability: the use of complex process control systems.

Process control systems (PCS) are industrial measurement and control systems used to monitor and control plants or equipment. They are utilized in numerous industries, including energy, manufacturing, chemical production and storage, food processing, and drinking water and water treatment systems. PCS are often referred to generically by one of the most prevalent types, SCADA, or Supervisory Control and Data Acquisition, but there are other types such as Distributed Control Systems (DCS).

These systems vary in function, size, complexity, and age. Some function in an automated fashion. Some rely on a human/machine interface, where the system provides critical information upon which an operator bases process control decisions. Some digital control systems can be "reprogrammed" from off-site through dial-up connections or through web-based access. This physical-cyber nexus creates a complexity which requires a comprehensive approach for protection.

Some methodologies for cyber and physical vulnerability assessments have not taken into account the implications of a process control systems failure on the operation or safety of the infrastructure. In addition, exclusively cyber, personnel, or physical security measures leave process control systems open and accessible. Protective measures must be responsive to all aspects of vulnerabilities regardless of the path for delivery and must keep pace with changes in technology.

SCADA systems were originally designed to be an isolated operational system with no outside path to access the system. However, competitive, economic, and technological pressures have opened these systems to corporate and vendor networks. Some SCADA networks have been joined to business networks with no air-gap technology emplaced and vendor networks have 24x7 accesses to critical SCADA systems for maintenance purposes. Moreover, both operating plant and SCADA staff use remote terminals for after-hour's maintenance via LAN or dial-up connections, leaving themselves open to cyber attacks. In most cases, remote terminal units can be accessed by anyone with a modem dialer. More often than not, systems will have no passwords, default passwords, or passwords as simple as "1234". Passwords are routinely left at the "out-of-the-box" default and rarely changed for fear of affecting critical operations.

To address the protection of these critical systems, IAIP has developed a comprehensive strategy to protect each element of process control systems. Our focus is on joint government-industry efforts to identify key assets, discover vulnerabilities, analyze risk, implement effective protective measures, conduct joint exercises and training, disseminate information, and develop inherently safer technology. Since most process control systems reside in the private sector, our ability to always effect change are sometimes affected by business factors that we cannot control.

IAIP manages this as a team effort that includes all parts of the Directorate, including PSD, the National Cyber Security Division (NCSD), the Infrastructure Coordination Division (ICD), and the National Communication System (NCS). The bulk of the remediation and protective activities are conducted by PSD and NCSD. To support these efforts, the Assistant Secretary for Information Analysis (IA), the intelligence arm of IAIP, along with the Office of Science and Technology, Office of State and Local Government Coordination, and the Office of Private Sector Liaison, provide the Office of Infrastructure Protection (IP) with crucial information and assistance. Beyond the Department, we are coordinating protection activities with the Department of Defense, the Department of Energy, and others. We are working on international partnership with Canada as it relates to the control systems of the North American electric grid.

In order to put this into perspective, I would like to briefly explain our overall operational philosophy. The overarching principle is to "Detect, Deter, Devalue, and Defend."

How do we do this?

- Through the deployment of specialized teams of security specialists to conduct site assist visits (SAVs), to evaluate vulnerability and establish whether or not site protection plans adequately address real-world security concerns.
- Through the development of community-based buffer zone protection plans (BZPP), that recognize that security does not end at the fence-line, and that local law enforcement and emergency responders are as integral to security as onsite personnel and equipment.
- Through third party submissions, including information provided from other Federal agencies, State and local governments, and private sector entities.
- Through special penetration testing of systems.

Immediate efforts focus on protective measures that can be implemented within the as-installed/legacy environment, such as inexpensive technical or procedural changes that can be implemented at the site and in the immediate future. Near term efforts include detailed testing and assessment of the vulnerabilities of PCS. In the long-term, we will work with the private sector on the development of inherently safer technology.

As part of PSD, we have established a Control Systems Section (CSS) that oversees the PCS Security program. CSS will identify and reduce vulnerabilities critical to domestic security related to PCS. This Section also includes the development and integration of the understanding of offensive capabilities, and providing relevant "hands on" operational support during DHS heightened security events.

PSD has identified approximately 1,700 facilities across the country that we hope to engage in a major vulnerability reduction effort during FY04. Of those sites, we have identified roughly 565 with process control systems. As appropriate, reduction in SCADA vulnerabilities will be undertaken just as reductions in physical vulnerabilities are.

Additionally, community-based Buffer Zone Protection Plans (BZPPs) that are being developed will incorporate protective measures for critical process control system sites. BZPPs, created through a collaborative effort between DHS, owners/operators, local governments, the law enforcement community, and other stakeholders, further strengthen identified sites by addressing the vulnerabilities of the larger community.

While PSD is working on vulnerability reduction at specific critical sites, NCSD is working the problem from a more global perspective. NCSD is holding meetings with industry experts to discuss in general terms vulnerabilities in a given critical infrastructure, participating in industry and government sponsored working groups, and directly engaging sector-specific Federal agencies, and State and local governments.

NCSD also analyzes and shares threat information of a cyber nature with all branches of government and industry. The Strategic Programs Section within NCSD routinely reaches out to industry, academia, and sector specific agencies to coordinated cyber protection activities.

Also, NCS is performing communications modeling of SCADA systems in partnership with Idaho National Engineering and Environmental Lab (INEEL). INEEL is the lead lab for the National SCADA Test Bed which is funded as part of the Critical Infrastructure Protection Test Range by PSD. The NCS Advanced Technology Branch has initiated a study to look at the SCADA vulnerabilities of the natural gas transmission systems serving the U. S. eastern seaboard and efforts are underway to identify the high power microwave vulnerabilities of commercial SCADA systems.

PSD and NCSD are actively participating with industry sponsored groups like the North American Electric Reliability Council's (NERC) Process Control Systems Security Task Force and the National Institute of Standards and Technology's (NIST) working group on process control systems security.

All of these activities will contribute to more comprehensive risk assessments of process control systems, including systems and component testing; will produce a refined, prioritized list of sites and vulnerabilities along with recommendations for effective protective measures.

In the long-term, targeted PCS security improvements will result in PCS architectures that are, by design, more inherently secure. This will be accomplished by ongoing partnerships with National Laboratories, owners and operators, and manufacturers.

In closing, I would like to reiterate first that SCADA vulnerabilities are a fact, just like a hole in a perimeter fence. The problem is that the SCADA vulnerability is not seen by the casual observer and therefore can easily go unnoticed. SCADA vulnerabilities are seen by those who would do us harm through their manipulation and it is incumbent upon IAIP to ensure that those responsible for protecting America are seeing them and doing something about it. Finally, as stated earlier, the Department of Homeland Security views this as a national effort involving many directorates within the Department and many organizations, both public and private, outside of DHS.

I would be happy to answer questions you might have.

Mr. PUTNAM. Thank you, Mr. McDonnell. Let me begin with one of the last things that you said—it is a national issue with many directorates of the Department of Homeland Security involved. What one directorate is ultimately accountable for the successful protection of this critical infrastructure?

Mr. MCDONNELL. Sir, I am the accountable executive at the Department of Homeland Security for this effort.

Mr. PUTNAM. OK. And how do you coordinate then with Amit Yoran and the cyber security folks?

Mr. MCDONNELL. Well, Amit and I both work for Bob Liscouski, who is the Assistant Secretary for Infrastructure Protection. We talk daily. This is one of the many issues we deal with. We are in the process of developing a joint package to understand how we both deal with each part of cyber. When you look at SCADA, we have Amit looking at the ones and zeroes, and that is how the hacker is going to come in, some guy sitting in an Internet cafe in Paris being able to hack in there or even locally coming in and affecting the code, rewriting the code. We also have to look at what are the systems themselves, how can they be intercepted. We are moving toward wireless technology, that has already been mentioned, and that adds another dimension of an avenue into the systems.

My teams when they are in the field look at all of the security considerations at a site. The vulnerability of their SCADA systems is one of the things that the teams look at. I have had teams just since the Department stood up the 226 sites around the country, as mentioned in my opening statement, we are going to be at another 1,700 during this year, at every one of those we are looking at the physical nexus for is there a control box that somebody can get into and tap into, are there wires set that use an induction system, you can get in and take over the controls.

So Amit and I have to work extremely closely to make sure we understand what each arm of the organization is doing. But we are doing it from a different level. He is at a global level, looking at how people are using the Internet globally, not just the Internet, but other malicious code types of attacks, where I am at the local level, looking at what is at the site, what are the vulnerabilities there that could be taken advantage of. It is an ongoing process. We talk literally all the time about this as well other issues.

Mr. PUTNAM. Thank you. The users of SCADA seem divided by their lines of business. The electrical industry does not necessarily talk to oil and gas industries, does not necessarily talk to the chemical industry. But according to the testimony provided by Siemens at our last SCADA hearing, SCADA systems are largely the same from industry to industry. What role does the lack of coordination within the private sector play as you work to solve these problems? I will begin with Mr. McDonnell and then go to Mr. Dacey.

Mr. MCDONNELL. Thank you, Mr. Chairman. When PD No. 63 was written back in 1997, infrastructure protection was stovepiped, so to speak. It was a Federal agency overseeing the care and feeding of all the different business sectors out there. So, for example, prior to the Department of Homeland Security, I was the Director of Energy Assurance. My responsibility was the energy sector, there was another department that had the chemical sector, Treasury had banking and finance, etc.

What has happened now with the President signing HSPD No. 7 several months ago and the creation of the Department is we now at the Department of Homeland Security are responsible for the coordination across all of the sectors, with all of the Federal agencies to ensure that the good things that are happening in one get to the others.

To your point, SCADA systems, there may be one manufacturer and maybe one patch that Nork found for the electric grid folks that may apply in the chemical sector. That is exactly the same in the other systems that we are dealing with out there. I may find a physical vulnerability that is common across many different business sectors.

So the way we are addressing that is my office produces common vulnerability reports. When I have teams out that are looking at these things, what are common in different sectors, at different facilities, and then how do we ensure that folks that need to do something about it can track those things down and see if they have the same problem and fix them. We will be doing that—and we do that to some extent in SCADA right now but it is still, quite frankly, in its early stages of development. I have a SCADA common vulnerability report in the works that I should see before too long that will just be part of the package along side chemical site security and other types of things.

The whole concept of this is the Department has to know where we have specific vulnerabilities. Then we have to pull back from where that specific vulnerability is, ask the question, where else are those vulnerabilities, and make sure that fixes that apply to a specific site in, say, New Jersey get to the guy in Florida or California that need the same information.

Mr. PUTNAM. Mr. Dacey.

Mr. DACEY. As we discussed in our report, when we were doing our work in research and talking to a lot of experts in SCADA field, the general consensus continued to come back that there needed to be more coordination. There are a lot of activities taking place. It, quite frankly, took us quite a bit of effort to try to put together all of the initiatives we described in our appendix because they were not readily available in one central place.

So I think in terms of the interest in the industry, there is an interest to get together because these SCADA systems share common vulnerabilities and common problems and some of the solutions, quite frankly, are common as well. So I think that is an important area and that is what led to our recommendation that the Department, in its role as laid out in the strategy to secure cyber space, put together a strategy for developing and coordinating those activities in one central place. And I am pleased to hear today that they are taking efforts to do that of late. Again, we have not been in and looking at the Department since we did our report, and I believe your section was set up sometime in December, if I recall. So it is good that action is taking place. It is a very critical element that needs to be carried forward.

The other part of that is the research and development. I think it is very critical that the folks that are affected by SCADA systems get together and try to sort out what research and development needs to be done and needs to be accomplished to help secure these systems, because, as you discussed in your opening statement and as we discussed in our report, there is some inherent insecurity in these systems and they do not have a lot of capacity to lay on encryption and things of that nature. So I think that is another area that needs to be looked at carefully, again through a coordinated effort, which the Department should be working with the private sector and other Government agencies.

Mr. PUTNAM. Do you have a breakdown, either of you, for what percent of SCADA systems are in private sector hands versus Government? But then within the Government, what I am concerned with is municipalities versus counties versus regional governments like flood control districts, water management districts, mosquito control districts, whatever, and States. If you are talking about a small county on the banks of the Mississippi River that is managing a very important piece of the flood control structure, that maybe the Corps does not have the money to upgrade SCADA systems, certainly, in south Florida we are dealing with it around Lake Okeechobee and the Everglades, control structures that are quasi-governmental. Do they even hit your radar screen, or are you really kind of focused on the bigger, more visible ones at this point?

Mr. MCDONNELL. Those absolutely hit our radar screen. The first part of the process in the Protective Security Division is what we call the asset identification shot. It is essentially a domestic targeting branch where we work with State and local officials, with private industry, with sector-specific agencies and say what are the things out there we should be concerned about protecting. We do that absent a vulnerability analysis initially because we need to know what are the things, the systems, the specific facilities, the systems of facilities, that, if affected, would have an impact that is unacceptable. Now we look at that in four different ways: First is public health and safety, what is the prompt effects of an attack on a facility; the second is economic impact; third is a symbolic nature; and fourth is national security, and that is the ability to support military mobilization and those types of things.

We are in the process, for example, of building a new set of data for fiscal year 2005 and fiscal year 2005 activities and we have had 13,000 items already submitted to us by the States after looking at their systems. I have a team, it is the Asset Identification Section, who is sitting down with their counterpart agencies and saying, OK, for example, that levee on the Mississippi, just for the sake of argument, it gets on the list, the State says this is critically important for crop protection, or it floods the town. It is incumbent on us then to help them identify what that is vulnerable to. It may be a physical attack or it may be a cyber attack. If it is a cyber attack, then the next step in the process is what can we do about it.

It sets up a process where we are actually going to operate, and we are operating now, based on if anyone thinks that something should be considered for protection, it will be considered for protection. How far down the road we go of actually implementing protective actions will depend on the analysis between that nomination of a facility for protective actions and the actual implementation of protective measures. Who does what protective measures will be a collaborative effort. We have inside the gate activities that need to take place, for example, where owners and operators have to do fixes, and we have outside the gate. A major effort underway now is to create buffer zone security plans. It is taking the operational environment away from the terrorists in the vicinity of the targets. We could build fences as high as we want and we could make a static security environment inside of a facility be impregnable or seem to be, but if we leave the area around it open for people to operate in, we leave the people vulnerable that are trying to protect our facilities.

It is exactly the same in SCADA. We have to know what is there. We have to know the ways a terrorist could get in. And then we have to figure out how we plug that hole, so to speak.

Mr. PUTNAM. Thank you very much. I would like to now recognize Mrs. Miller for 10 minutes.

Mrs. MILLER. Thank you, Mr. Chairman. Mr. McDonnell, if I could followup a bit. I tried to take some notes there. You were saying that the DHS had identified about 1,700 different facilities thus far. Did you actually do that work yourself? How did you coordinate and cooperate with the States? Now it is my understanding that each State was responsible to deliver to DHS a State plan, their own assessment plan of the kinds of soft targets that they might find within their respective States. So I guess my first question is, did you actually do that work, or was that done by the States?

Mr. MCDONNELL. It was done in combination. The plan that the States had to submit was due in at the end of December of this year. For the grant process for putting funds out to the States in the fiscal year 2004 appropriations, we were required by October 15 to brief leadership on the Hill of what we were going to use for infrastructure protection grants and what strategy we went through picking facilities. So we actually this year had to pick facilities pre-dating the inputs that were coming in through the strategic planning process that the States were in the process of submitting.

Now that being said, what we did is, over the last year we have collected a lot of information, we have consolidated that into a list. I then took that and I met with the Homeland Security advisors and I said here are the 1,700, what do you think? For example, there was a shopping mall that ended up on there that was in the Meadowlands in New Jersey that does not exist yet. It is licensed, you look at all the business records and it shows that it is there, but nobody got around to building it. So we decided to take that off. We are not going to pour a lot of protection into that. But it was critically important in that case because Syd Casper, in New Jersey, said, hey, Jim, we do not have that here, but there is something else there that does need to be protected. And so it is an iterative process.

I think, quite frankly, it is going to be another probably two cycles before we really have a very good handle on all the different things that are out there that need to be protected. But it is going to take continuous dialog. Hearings like this are good. Any time we can get people together to talk about this and get people thinking about getting the information back and forth so we can put good plans around things, I think we win.

The 1,700 sites will probably, by the time we get done with this cycle with the State, be closer to 2,000 for actions during this year. We already see a little bit of a bump up. They are not the top 2,000 critical sites in the country, per se. But a big part of it is soft targets. We are putting a lot of effort right now into those areas that do not have any protection and looking at places where people are gathering and we could have low level attacks outside of the critical infrastructures, stadiums, shopping malls, those types of things. So there is quite a bit of movement in that area as well as the traditional sites. Included on the list at the top tier are chemical facilities, the most hazardous facilities, nuclear plants, rail, bridges, those types of things. And of that 1,700, there is somewhere in the range of 560 that have digital control systems that, as we put these buffer zone plans in place, will be part of the consideration.

Mrs. MILLER. Have all the States complied? Where are you nationwide? Have all the States complied with the requirement to have their State plan in? And then when they were doing their State plan, did DHS actually set a criteria? I mean, if you have some State telling you you are going to have a shopping mall in 5 years and they have that on their plan as opposed to an existing nuclear facility, there should have been some criteria as the States were doing their own assessments I suppose.

Mr. MCDONNELL. Right. I will have to get back to you on the specific number. I know we are very near everyone having submitted those.

Quite frankly, the process that we used in asking the States to do the submission pre-dates the development of the division that I run and a lot of the other parts of the Department. What we did not want to do was, the States were pretty far down the road getting a strategic plan done, and so we did not to stop them and ask them to start all over again. So that process has continued. What we did in parallel is engaged with the States to say now let us start talking more specifically about what criteria we want to use for identifying critical infrastructure and then how we go forward with that.

So it is an ongoing process. We have the dialog underway, we have common goals and objectives, we still have to work out details as far as what is the best reporting scheme going to be, how do I make sure that one State looks at things the same way another State does. Honestly, they are going to look at them differently. I have to understand their perspective and figure out how I support them and try to get a national picture.

Mrs. MILLER. There has to be a standard I think. And the States have to look to us, the Federal Government, through you, to set those standards. And I asked this because you also mentioned about grants to the States. My State of Michigan I am aware has submitted their plan, although I do not know what the plan looks like. We have been told it is not for us to see, quite frankly. So I am hoping the plan is fine. We did have Secretary Ridge in my district most recently, and we were talking about appropriations to DHS based on some of the criteria as the States were doing their assessments.

I guess I would ask you if you have any comment on this. For instance, in regards to some of the grants, a big part of the criteria there is based on population, which makes sense at first blush. But we have a situation in my district. As I mentioned, Secretary Ridge came in and we took him on a helicopter tour—if you can think of Michigan as a mitten, I am talking about this area here, which is the St. Clair River. We share a very long liquid border with Canada there and we have the third busiest border crossing on the Northern tier there called the Blue Water Bridge, which is the only commercial corridor on the Northern tier that can accept hazardous material across, unlike either Buffalo or the Ambassador Bridge in the city of Detroit. We have the CN rail tunnel there. We have what we call chemical valley. Sarnia in Canada there has a number of chemical plants across there. And yet this is a county that has a very small population base but, obviously, some unique characteristics in regards to a soft target. So I do not know if you are able to assist in this, but I certainly want to keep talking about that, that the criteria for the grants has to take into consideration a much more global perspective I think. And it is so important that your Department continues to work with the States. So I guess my question would be then, when you get these plans from the States, what are you doing with them?

Mr. MCDONNELL. What we are doing now with the States is we are actually taking their inputs, we are refining what the lists are, and then we are going out and providing them support for buffer zone security planning and so on. The population and population density piece of the formula was used in the Urban Area Security Initiative which, by definition, was focused on the large cities. The selection of critical infrastructure assets for the other grant programs and the activities that my division is leading does not consider that they have to be in a city.

So what I would expect in that case, and I will go back and check on the Blue Water Bridge, is I would expect the Michigan Homeland Security advisor, if that was not already on the list, would come back and say, hey, you need to add this, and we would do so. And then that would just be part of the process of my teams would be working with the State and assisting the State in developing those security plans, identifying where we can help, and just doing a better job nationally of dealing with the problem.

Mrs. MILLER. I just keep going on about setting the standards. I think it is so important that the Federal Government, through your agency, sets the standards, whether it is for as they are making their analysis throughout the States for their soft targets, or whether they are talking about setting up communications systems in all the various counties. The Secretary and many others have mentioned and almost everybody has agreed that is a priority in every county, right? Every municipality has such antiquated communication systems and everybody is running around trying to get grant money to put into communications systems to talk to one another. There is sort of a lack of standards, I think, on communications towers, all of these things. So I mention that to you as well.

Once you have identified, and I do not know if you have gone this far, but as you have assessed where all of your soft targets are and that, how will you provide oversight for the States? How does that part of it work? Would you do that from a centralized location, from Washington? Would you do that through your proposed regional homeland security centers through the DHS? Do you have any next step there on how you would oversight that?

Mr. MCDONNELL. Yes. I would use the term verification as opposed to oversight in that I am not directing the States or sort of telling them what to do. It is more of an assist role. And that being said, it is very effective. I do not have any real problems in dealing with the States in that area.

I inherited a program from the FBI in the transition called the Key Asset Program, which was a field agent in all 56 of the field divisions who was responsible for critical infrastructure protection. I am in the process of hiring new replacement agents to be in the Secret Service offices throughout the country who would do sort of the daily care and feeding of those sites. This is very similar to the way MI–5 does it in the U.K. I went over and worked with those guys quite a bit to figure out how they handled this on a national scale.

Say the person I have in Detroit will have a set number of sites, jurisdictions they have to work with. Their job will be on a daily basis to visit those places, talk to them, see how things are going, identify if vulnerabilities have been plugged, just spot checking, if you will. And those folks, prior to the regional offices being stood up, will report directly to my office at headquarters. I have a Secret Service agent detailed to me to manage that. And then over a period of time, as the Department's regional offices mature, we will have protective security detachments in each. Right now, everything is being run out of headquarters because I do not have regional and local activities yet. But as that evolves, then those local guys will work for the regional folks who will work for our headquarters policy oversight shop in Washington.

But we really want the protective security activities to be community-based activities, much like the disaster recovery. The security at a site is not just the company, it is not just the local sheriff or law enforcement, it is a team effort and everybody has to be part of that team. So we are trying to push these activities to the local level. And this again gets to the difference between Amit Yoran's organization looking at global activities where there are not people necessarily local, to my shop really working at boots on the ground, talking face to face, knowing the people, having a relationship, and being able to be a reach-back capability for those local folks that need help.

Mrs. MILLER. Just one more question. Both of you gentlemen are trying to talk about what the necessary safeguards would be. Obviously, we are talking about dollars here, whether that be a local municipality, local sheriff's department, or whether it is a public utility, or what have you. Do you have any ideas at all about how the private sector might try to pay for some of these things? A utility, for instance, would have to go through their State's public service commission, that is what we call it in Michigan, I do not know what they call it in every State, to look for rate increases. Or do you think that some of these utilities or what have you would be looking to the Federal Government to set sort of a standard, some way of recouping some of these costs? Are you thinking about that at all or getting any feedback on that?

Mr. DACEY. In terms of working on our report, again, the message we heard consistently from a variety of sources, vendors of SCADA and control systems, industry representatives, was a concern that it may not be economically feasible for them to proceed and invest the additional dollars in control systems security. And as a result of that, some of the vendors indicated they were not promoting heavily advances in that area. So we heard that a lot. Again, this is assertions that were made to us by a wide variety of people.

But I think the issue becomes what level of security is appropriate. Some of the efforts that are underway to do research and development to develop standards and some kind of a basis for expectations, if you will, on what should be done to secure these technologies I think would be helpful out there. And then it becomes upon the private sector and the States to determine whether or not they are going to be financially able to afford whatever that level or standard might be. And I believe in the strategy it talks about the Department coordinating with the private sector to work on developing some type of standards. So I think that is an important area.

We reported in the past, relating to CIP and general critical infrastructure protection, that the Department now needs to look at and consider the need for public policy tools to determine whether or not they are going to be necessary, whether it be grants, tax incentives, or whatever might be appropriate, to consider the need for those to provide additional incentives for the private sector to proceed. There have been a couple of situations where EPA has provided funding to do vulnerability assessments at water treatment facilities for major municipalities, for example.

So there has been some activity. But what we had recommended was more of a broad based needs assessment to try to figure out what would be the best incentives for the private sector and State and local governments. But part of that I think is really setting an expectation about the level that needs to be attained and whether or not they are willing to do that without additional public policy tools.

Mr. MCDONNELL. Just to followup on that. As I mentioned, I was at Energy Department before I started the office at Department of Homeland Security. In my 2½ years, my experience has been that corporate leadership wants to do the right thing if they are given the right information. And, quite frankly, the Federal Government becomes a holder of the information quite a bit.

And a big part of what we are seeking to do at the Department of Homeland Security is build the pipes to get the information out to people so they can make intelligent decisions. We need to get the specifics of SCADA vulnerabilities, for example, out of rhetoric and into, hey, here is a specific thing that is out there. One way to do that is the development of standards. We are working with the American Society of Mechanical Engineers, for one, to help us develop industry-based standards for risk assessment in the various sectors. SCADA will be a part of that.

The other is setting expectations. One thing that we can help to do, and we are exploring this right now, is something like a DHS seal of approval, an underwriters laboratory, if you will, for if somebody comes out with a new software package for digital control systems, it goes to our test bed, the guys take a look at it and they say here is an assessment of it. I think from a business model, what you end up with then is you have a vendor who says, hey, this has been vetted, they have looked at this based on knowing what the vulnerabilities are, what the adversaries might try, and I am selling you something that is secure. The corporate executive then can go to his board and say, look, we are making the right decision. It frees them up from litigation for not using due diligence. There are good ways to build this but we have to build a baseline where there is actionable information in the hands of the executives and decisionmakers in the companies and an option. If we can move toward a particular system, and we are not saying this is a better system than this one, it is just an honest assessment of its vulnerabilities versus another, then that company can say I am going to buy that one and not the other. And I think that starts driving the business case for across the board improvement in security of the systems.

Mrs. MILLER. Thank you.

Mr. PUTNAM. Thank you, Mrs. Miller.

Let me followup on her line of questioning about standards and assistance. I do not know that I ever got an answer on the breakdown of municipal, State, county versus private sector so that we have a handle on who is actually going to be responsible for paying the bills. But once you have this 1,700 list finalized, then presumably we would have the price tag for bringing them into a higher level of preparedness or security. So then the question is who bears the cost. And if it is the private sector, and we know that 80 percent of the critical infrastructure is in private hands, then they are expected to bear the cost, but they are not mandated to bear the cost. Is that correct?

Mr. MCDONNELL. In most cases, yes, sir.

Mr. PUTNAM. So if they are presented with the options, as you illustrated, of a more secure system versus a less secure system, or upgrading versus not upgrading, there is no compulsion to act in the law. Is that correct?

Mr. MCDONNELL. I think that is fair if it is strictly a question of investment. So, say, if I come in and say you have a whole year, if you do not fix it, somebody might attack you, and they say, yeah, yeah, whatever, thank you very much, I am not going to do anything about it anyway, what my experience has been to date is that is not a real problem right now. Now it may be a problem that evolves over time, but people are very, very sensitive to being vulnerable to attack. Some of the fixes that we are talking about are literally unplugging a phone line. Not all of the fixes are very complex.

The key is to make the decisionmakers aware of where they are vulnerable. That is where the nexus between the Government operations, understanding the intelligence that is out there, the threat that is out there, and the vulnerabilities of the systems, and then being able to look a corporate executive in the eye and say you have this vulnerability, I am on record for telling you you have it, that it is your choice whether you do something about it right now, but if you do not, you are liable to be dealing with regulation down the road, if you do not, you are liable to be dealing with litigation if something goes wrong. So there is a coercive element to this.

Now, that being said, in the energy sector, for example, the FERC has a lot of ability to help push these types of things. There is a question about rate recovery. The FERC, for example, can put out a rule that says if you are going to operate in the interstate transmission of electricity, here are some minimum standards that you have to follow, and then can encourage the State public utility commissions to allow rate recovery for those activities.

Mr. PUTNAM. That is true. They are a legal monopoly and they have a price fix regulated by State legislatures or FERC or whomever. But what if it is a private chemical company that does not have the benefit of all of that and they have to make decisions about their bottom line? And in the real world, as you know better than any of us, the threat matrix is changing every day. You find some scrap of paper in a cave and it has got a picture of a chemical plant. The next week you find a picture of a dam. The next week you find a picture of a bridge. And you are expecting businesses, if you go make this pitch, well, this week is chemical plant week, or next week is bridge week, and next week is tourist attraction week, then how do they really make informed decisions.

And correct me if I am wrong, there is no safe harbor. You were using this liability issue as a threat, that I am on record telling you that you have a vulnerability, I am telling you this is a problem, you can act or not act. If they choose to act, is there a reward by saying we put them on notice, they made use of the best practices and technology of the day, therefore they are protected?

Mr. MCDONNELL. I think, as you point out, it is extremely complicated in how we actually push this down the road. It really gets to what is the consequences of failure. If, in fact, a dam, for example, has a SCADA vulnerability that we identify that risks the lives of thousands of people, I think with that piece of information it is pretty easy to ensure that dam does something about it.

Mr. PUTNAM. OK. Let's stop right there.

Mr. MCDONNELL. Sure.

Mr. PUTNAM. Perfect example. Who pays for it? It is a county in the Midwest or in south Florida in the middle of the glades, their total county budget is $30 million a year and it is going to cost them $5 million to fix the dam. Who pays for it?

Mr. MCDONNELL. I have the ability to sit down with the State Homeland Security advisor and say you need to take some of that grant money and fix that problem at that dam. And we have done that. So there is a process. There is plenty of money in place to do specific things. Now where you run into a problem is when people say, well, the sector needs to be fixed. Well, not all the dams are equal. All the dams may have the exact same problem but what we have to do is say that is an unacceptable risk. It is a risk-based decision, it may be a public health and safety decision, but we can find a way to fix it when we get to that specificity. And that is the challenge for our organization is to get to that specificity.

Mr. PUTNAM. Here is my couple of concerns, and then I need to move to a few other questions that we need to get down for the record. But human nature being what it is, and the threat being as complicated as it is—and it is far more complicated than us just saying we are going to go make everything prepared for any threat. It just does not work that way. You have basically identified 1,700 sites. You and your colleagues around the country and in the States have basically said there is a top 1,700 list. My thinking, being a little bit cynical, is that the people who did not make the list are going to say, oh, but wait, we are vulnerable too. Look at all these things that we have that we need grant moneys to fix. Just like every police department in America wants to have first responder equipment equal to and greater than New York and L.A. and Washington. I mean, you see it. It is a feeding frenzy.

I see there are certain sites particularly that meet Category III of your rubric, which are symbolic sites, that probably would just as soon not be there. But I can see a lot of sites saying, hey, this is the spot we need to be in, we cannot even afford to meet EPA water quality standards now because we have a plant that was built in the 1940's, but if we say that we are at risk of poisoning a half a million people, we will get a brand new sewer treatment plant, or we are going to get a brand new weir, or we are going to get a brand new whatever. So that is my concern in the real world process of how all this stuff works. And it is never ending because you cannot be more prepared than the terrorists' imagination.

And I commend you for making a first step by saying these are the top 1,700, 560 of them have process control systems. At some point I hope you will be able to say the price of bringing these to an acceptable level is X amount. You, Congress, can decide whether you want to do it all in 1 year, whether you want to put it on a 5-year phase-in, but that is our call to make. And put it on sort of a milestone and task-oriented funding plan. But those are my concerns.

The other issue is that GAO says in their report that these are the folks involved in SCADA security—DHS, Energy, Defense, 5 different national labs, EPA, FDA, NIST, 2 multiagency working groups, the NSF, 11 private sector groups, and 1 government-private partnership, for a total of 26 players. How does all that work, Mr. Dacey?

Mr. DACEY. That gets back to our recommendation again. Sorry to get back to that, but the bottom line is that is what we recognized is that a lot of these efforts were initiated independently of each other. It was a need recognized by that particular group or sector to deal with a specific issue. DOD did work on determining what the effect of weaknesses in SCADA had on their ability to carry out military operations. And each one had its own genesis. That is why there is a need to coordinate these efforts so that we are getting the most leverage out of the activities and resources that are being put into this to get to the best answer as quickly as possible. I think that is a key issue in coordinating these efforts, again, something we heard consistently throughout discussions with those.

Mr. PUTNAM. We wrestle with this on corporate information security and we put together a working group and we spent several months working through all those issues. It came about as a result of industry saying there is not any one law that you can pass that is going to solve this, it has to be collaborative and it has to be voluntary, and we need to have this underwriter's laboratory type model, very similar to what you are talking about for SCADA. But at the end of the day, there has to be some compelling reason for everybody to work and play well with others. I do not know what the proper formula there is, whether it is a safe harbor in the liability issues, whether it is tax credits, or whether it is just a cold hard law, but these are the issues we have to deal with to make these systems more secure.

Mr. McDonnell, both the Science and Technology Directorate and the National Cyber Security Directorate at DHS have initiated several activities in the area of SCADA security. How are you coordinating their efforts? We talked about the 26 outside of there. Even within DHS you have all this going on. Do you expect there to be one overriding plan that comes out in this SCADA vulnerability report that you referred to earlier?

Mr. MCDONNELL. Yes, sir. We are in the process of taking the President's Directive on Infrastructure Protection, HSPD No. 7, and putting in place now how we operationalize that across all the sectors, across all the departments, and truly build a national plan. It is our intent that SCADA activity will be working to a common goal through a common process. Now, there will always be outside of government competitive folks out there that want to be doing their own thing. That being said, we absolutely are starting to pull all that stuff together and we will have a single national effort led by the Federal Government for SCADA.

It is going to take some time to pull all this in. As my colleague mentioned, there are some equities in there, Defense, for example, has very specific reasons for looking at SCADA, the Department of Energy has a totally separate shop that is looking at SCADA and the processes in the nuclear control systems at the laboratories, the nuclear weapons processes, and they are never going to just kick that into a big interagency collaborative effort. But what we do have to make sure is that we understand what is going on in these sort of compartmented areas and we are not duplicating effort, that I am not paying for an R&D program that kicks out something that has already been invented over at the Defense Department but I just did not know about it. So that is absolutely part of the plan, sir.

Mr. PUTNAM. As you know, we have a very open records policy in this country and even more openness depending on the States that involve the availability of design and blueprints, specific site locations, wiring configurations, frequencies. Could each of you speak to the risk or the lack of risk that is associated with public access to this type of information.

Mr. DACEY. Certainly, there is definitely increased risk when there is more information about the security of specific systems that people could use. If you look at some of the stuff that is on the Internet, there are operations manuals, there is just a lot of information out there that is publicly available to understand how these systems operate and what is being done with them. There are even many other sites, vendor sites which even tell you where their equipment is installed and how it is installed, or at least a general idea of how it is installed. So there is a lot of information out there that could be used by someone if they wanted to do some damage to learn and prepare themselves for a potential cyber attack on SCADA systems.

I think that combined with some of the other risks we talked about, such as the combination of these networks with other enterprise networks, exposes a real threat for hackers using just general purpose hacking tools to get into a network that is in one of these companies and use that opportunity to then get access to the SCADA systems if they are not compartmentalized and secured. That is where we saw in the Davis-Bessey plant where, as you mentioned in your opening statement, there a worm, the slammer worm migrated apparently from a vendor system through a trusted VPN, if I recall, right on into the nuclear power plant's main enterprise system and interfered with the traffic running in the control systems. So you have real issues there.

So you combine the two with the fact that you can go in, there is clear text going across these things, it does not take a lot of imagination to think someone who is really studying and intent on doing something could not start to get a pretty good understanding of how these systems work, how the messages flowed, what they look like, and so forth and so on, if they could get into these systems. So I think there is a real risk. But it is not just the fact that the data is out there and available, that it is the other things which are really compounding that risk I think.

Mr. PUTNAM. Does the access to information present a risk such that we should consider policy changes to public access to those plans and designs and operations and sites?

Mr. DACEY. A lot of these systems, particularly newer ones which are moving to some of the common protocols, communication protocols and networks that we see out there and using the Internet as well, I think a lot of that information is public knowledge now. I think the bigger key is to better secure these networks and systems so that people cannot get to them through defense in-depth and other means. In other words, if a lot of these systems are adopting these current technologies, it does not take a lot to imagine getting in. Even if the information was not out there, one could still get in and gain a lot of insights if you could break into these systems. So I think the real key gets back to protecting the systems adequately so people cannot get in and start looking at traffic, you know, so-called sniffer software you can put in if you break into a system that looks at all the traffic going through, and you can use those to identify a lot of information on specific traffic that the control systems are using. So, again, it would help if that were not there, but I think there are a lot of other issues that need to be addressed that are just as important, if not more important.

Mr. PUTNAM. Mr. McDonnell.

Mr. MCDONNELL. Yes, sir. You asked specifically about change of public policy. Within the Homeland Security Act was the Critical Infrastructure Information Act, and that does provide an avenue for a company to submit information to the Department of Homeland Security, have it stamped as critical infrastructure information, and it is exempt from FOIA. And it is preemptive legislation and it is therefore exempt from State sunshine laws and so on. So there is an avenue for newly submitted information.

Mr. PUTNAM. Prospective.

Mr. MCDONNELL. Yes, sir. But once a barn door is open, it is open. There is an unbelievable amount of information that is available out there. You cannot get it back. The best thing that we can hope for is more discipline in what gets put on Web sites and controlled. And over time, a good operational security program will have better and better controls on those critical information. Quite frankly, if someone has information out there already and they have to go back and do something to change it, they have to physically change the system, they are not going to get the information back. The only way to mitigate that. My worst nightmare is somebody doing all of their planning from an Internet cafe in Paris. They can sit overseas and look at the floor plan of a chemical site, see what kind of control system it has, see what defenses look like, see what the local response capabilities are by going to the city's Web site. We have to influence that and we have to do that by the originator stopping posting public records, management, those types of things. So we have to identify the information we want to protect, and we do have a way to protect it now, but it is going to take some time to get people to sort of turn that and start putting it into the system.

Mr. PUTNAM. When I was a kid, which was not all that long ago, but you would go to the encyclopedias. And you can go to the Internet and you get the encyclopedia and learn how to build a bomb. That does not mean you could actually build an atomic bomb just because it showed you how to do it. But today, you are talking about not just the chemical plant or the nuclear power plant's blueprints, which I think, frankly, are inherently fairly secure by their nature, people knew when they built a nuclear power plant long before Al Qaeda that it was something that needed to be protected, but rather the isolated valve 12 miles away, or switching station, or router, or whatever that is in the middle of nowhere with maybe nothing but a chain link fence around it, if that. That is the kind of stuff that concerns me, not a $50 million factory or facility or whatever. Anyway, that is what bothers me about the access. And I appreciate your input on that.

According to your testimony in October 2003, the Science and Technology Directorate began a study of the current security state. When do you expect that study to be completed, Mr. Dacey?

Mr. DACEY. Let me check my notes. I do not recall if we have a date for when that statement of work was supposed to be concluded.

Mr. PUTNAM. And Mr. McDonnell, are you aware of the study?

Mr. MCDONNELL. Not specifically, no, sir.

Mr. DACEY. The statement of work called for delivery on about 90 days after beginning performance with an interim draft report, with a final draft report about 150 days after beginning performance. So that is kind of a general timeframe. So you are talking about 5 months. And I am not sure exactly when the study began.

Mr. PUTNAM. Mr. McDonnell, are you more concerned about, with regard to SCADA system threats, not everything else that is on your plate, do you worry more about an international threat, as you put it, from an Internet cafe in Paris, or do you worry more about domestic home-grown type threats?

Mr. MCDONNELL. I think international.

Mr. PUTNAM. Mr. Dacey, do you have an opinion on that?

Mr. DACEY. I think they are a significant threat. The thing I would add to my prior statement too is that there are not that many types of different control systems out there and they are used throughout the world. So it would not take much for someone potentially to get access to someone who had significant knowledge of operating systems in other countries that might be available to assist in some kind of attacks that might occur.

But it could be virtually anywhere. If you look at some of these SCADA systems for some of the large institutions that carry them out, you will see that for operational purposes and better management a lot of these SCADA screens can be pulled up from virtually anywhere in the world. Now several of the institutions we talked to have implemented stringent controls to authenticate everybody going in there. But, quite frankly, it is conceivable that if it was not secured and you broke into the system, you could literally see right in front of you the operator's screen for the SCADA system. It is a frightening thought.

Mr. PUTNAM. The DOE has not adequately funded the SCADA test bed. Is this something that DHS plans to fund, or is it still limping along in Energy?

Mr. MCDONNELL. That is something DHS intends to do.

Mr. PUTNAM. OK. Mrs. Miller, do you have additional questions?

Mrs. MILLER. I do not.

Mr. PUTNAM. We are expecting votes between 3:30 and 3:45. So at this point, I would like to excuse our first panel and seat the second one as quickly as possible and at least begin testimony before we have to leave to vote.

Gentlemen, I want to thank you for your responses and your candor and your interest in this very important issue. The subcommittee is grateful for your testimony.

Mr. MCDONNELL. Thank you, Mr. Chairman.

Mr. PUTNAM. With that, the committee will stand in recess. The first panel is excused. We will seat the second panel as quickly as possible.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene.

We will seat the second panel of witnesses and move immediately into the administration of the oath and then we will get into your testimony.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of the witnesses responded in the affirmative.

I will precede my introduction of our witnesses by saying that we are expecting votes very shortly. We would like to ask you to keep your remarks to 5 minutes. We will undoubtedly be interrupted for votes. I believe we have two votes, so we should be away for approximately 30 minutes and will return immediately. So we apologize beforehand. We will keep things going as quickly as possible.

Our first witness for the second panel is Joseph Weiss. Mr. Weiss is an industry expert on control systems and electronic security of control systems, with more than 30 years of experience in the energy industry. He serves as KEMA's leading expert on control systems cyber security. He spent more than 14 years at the Electric Power Research Institute where he led a variety of programs, the last of which was cyber security for digital control systems.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENTS OF JOSEPH WEISS, EXECUTIVE CONSULTANT, KEMA, INC.; DAN VERTON, SENIOR WRITER, COMPUTERWORLD MAGAZINE; GERALD S. FREESE, DIRECTOR OF ENTERPRISE INFORMATION SECURITY, AMERICAN ELECTRIC POWER; AND JEFFREY H. KATZ, ENTERPRISE IT CONSULTANT, PSEG SERVICES CORP.

Mr. WEISS. Thank you very much. Good afternoon Mr. Chairman, Ranking Member Clay, and members of the committee. I would like to thank the subcommittee for your commitment to a comprehensive examination of cyber security of the control systems utilized in our Nation's critical infrastructure. I also want to thank you for the opportunity to be here today to discuss this very important topic. My remarks will provide details on one, control systems design considerations and cultural issues; two, control systems cyber vulnerabilities; and three, key activities that need to be addressed and funded to secure control systems.

Control systems form the backbone of our critical infrastructures. A control system controls a process such as regulating the flow of water in a power plant or opening a breaker in a substation. I have been working with the key organizations that have a role to play in this area, including the Government, end-users, equipment suppliers, standards organizations, and others, none of which have been adequately coordinated. My formal testimony has been reviewed by representatives of DOE's Office of Energy Assurance and the National Energy Technology Lab, DHS' Cyber Security and Protective Security Divisions, the Idaho National Lab, the Sandia National Lab, the General Accounting Office, Carnegie Mellon Software Engineering Institute, the United Telecom Council, and a utility member of the NERC Critical Infrastructure Protection Committee which is responsible for issuing the utility industry cyber security standard.

Cyber security has been viewed as an information and IT, or Internet, concern. The basic design assumptions inherent in control systems are they would be stand alone and all control system users would be trusted users. However, competitive pressures have forced businesses to interconnect office and electronic commerce systems with control systems. This has exposed control systems directly to the Internet, Intranets, and remote dial-ups. Additionally, there is also a tradeoff between security and control system performance.

There are only a handful of control systems suppliers and they supply industrial applications worldwide. The control systems architectures and default passwords are common to each vendor. Consequently, if one industry is vulnerable, they all could be. Additionally, utilities in North America and elsewhere are able to obtain the source code for electric industry SCADA systems.

There have been more than 40 cases where control systems have been impacted by electronic means. These events have occurred in electric power transmission and distribution systems, power generation including fossil, hydro, gas turbine, and nuclear, there have been three commercial nuclear plants with denial of service events, water, oil, gas, chemicals, paper, and agribusiness. Some of these events have actually resulted in damage. Actual damage from cyber intrusions have included opening valves resulting in discharge of millions of liters of sewage, opening electric distribution breaker switches, tampering with boiler control settings resulting in shutdown of utility boilers, shutdown of combustion turbine power plants, and shutdown of industrial facilities.

The traditional Internet vulnerability tracking organization, such as the Computer Emergency Response Team [CERT], SANS, and the Computer Security Institute, are focused on traditional Internet and business system exploits and damage. The events and statistics quoted by these organizations do not specifically address control systems. Additionally, none of the control system impacts have been identified by these organizations. This lack of awareness is keeping executives from identifying cyber security as a business imperative.

This also results in a quandary, as you brought up earlier. Control systems suppliers are not building secure control systems because they do not believe there is a market, and end-users are not specifying secure control systems because they do not exist and would be more expensive. This lack of awareness concerning control system vulnerabilities and impacts is a gap that needs to be addressed.

Consequently, DOE's OEA tasked KEMA and Carnegie Mellon's CERT/CC to perform a scoping study for establishing a CERT for control systems, which we called e-CERT. The funding for establishing and conducting the e-CERT function would be approximately $3 million a year. The investment would substantially improve the reliability and availability of the critical infrastructure as well as providing the awareness necessary.

Existing cyber security technology has been developed for business functions and the Internet. Control systems require a degree of timing and reliability not critical for business systems. Because of this, employing existing IT security technology in a control system can range from lack of protection to creating a denial of service condition in and of itself. This has actually occurred in attempting to employ encryption in control systems. We do not know the true vulnerabilities of control systems. Penetration testing of business and control systems can lead to system interruption or require the system to be rebooted. Consequently, this testing must stop at confirming control systems can be accessed.

The National SCADA Test Bed allows vulnerability testing of control systems to help identify the actual vulnerabilities. This testing will also enable test bed personnel to identify the necessary technologies to mitigate the vulnerabilities. Several suppliers of SCADA systems have already provided systems to the test bed. Adequate funding is lacking, however, to enable the test bed to function in a complete and timely manner. A significant multiyear investment is required, and you will hear from others as to what those estimates are.

In summary, there are two key areas that require modest funding to help secure control systems throughout the industrial infrastructure—e-CERT and the National SCADA Test Bed. If these two activities are adequately funded, they can address awareness, minimize vulnerabilities, and evaluate and develop technology to secure control systems. This will minimize the threat of extended blackouts, like what happened on August 14th, and impacts on industrial production which will have a positive impact on the quality of life and security of the American population.

Thank you for your time and interest. I would be happy to answer any questions, including about industry coordination.

[The prepared statement of Mr. Weiss follows:]

Testimony of
Joseph M. Weiss
Control Systems Cyber Security Expert

before the

House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
U.S. House of Representatives

March 30, 2004

Control Systems Cyber Security—Maintaining the Reliability of the Critical Infrastructure

Joseph M. Weiss, PE, CISM
Executive Consultant, KEMA, Inc.

Good afternoon Mr. Chairman, Ranking Member Clay and Members of the Committee. I would like to thank the Subcommittee for your commitment to a comprehensive examination of the cyber security of the control systems of our nation's critical infrastructure. I also want to thank you for the opportunity to be here today to discuss this very important topic with you.

My remarks will provide details on:
(1) Control systems design considerations and cultural issues;
(2) Control systems cyber vulnerabilities, and
(3) Key activities that need to be addressed and funded to secure control systems.

On July 24, 2002, I testified to Congressman Steven Horn's Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. At that time I stated that since September 11, 2001, the focus of security in the United States has been on physical terrorist attacks. Cyber security focus has been directed towards Internet use and networking technology. Dramatic steps are being taken to ensure security against physical attacks and increased emphasis is being placed on securing the Internet and networking systems for traditional IT business systems.

However, the same cannot be said for operational control systems, which are at the heart of our critical infrastructures and endemic across many industries. Control systems include distributed control systems (DCS) and programmable logic controllers (PLC) – also referred to as process control systems (PCS) - and supervisory control and data acquisition (SCADA) systems. These systems are crucial to the operations of, and form the backbone of, the global industrial infrastructures. The industrial infrastructures include electric power, oil and gas, chemicals, pharmaceuticals, water, paper, metal refining, auto manufacturing, transportation, and food processing to name a few.

It is important to note that there are a limited number of operational control systems suppliers, and the same systems are sold virtually in every country throughout the world.

There is a growing threat of cyber attacks on operational control systems that could create a crisis for which no country, company, or person is adequately prepared. Based on my knowledge of, and experience with, control systems I believe this is a very real possibility. I will provide several recommendations on how the government can help secure our nation's critical infrastructures from intentional and unintentional cyber events.

I am involved in a number of organizations and activities that have provided me insight, expertise, and a working knowledge of the cyber security issues we face as a nation and as a world community. I am a member of many active groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council 's (NERC) Critical Infrastructure Protection Committee (CIPC), ISA's SP99 Manufacturing and Control Systems Security Committee, and the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF). I would like to state for the record that the views expressed in this testimony are mine. I am not representing any of the groups in which I am involved.

I also would like to add that representatives from the following organizations have reviewed this document: Department Of Energy's (DOE) Office of Energy Assurance and National Energy Technology Laboratory, Department of Homeland Security's Cyber Security and Protective Security Divisions, Idaho National Engineering and Environmental Laboratory, Sandia National Laboratory, Government Accounting Office, Carnegie-Melon's Software Engineering Institute (CERT/CC), United Telecom Council, and a utility member of the NERC CIPC.

Abstract

Control systems have been designed to be efficient, rather than secure. These systems are used throughout the industrial infrastructure. To date, there have been more than forty cases where control systems have been impacted by electronic means. These impacts have included damage to systems and the environment.

In order to better secure the control systems controlling the critical infrastructures there is a need for the government to support industry in two critical areas:

- ***Establish an industry-wide information collection and analysis center for control systems modeled after CERT*** (Computer Emergency Response Team) to provide information and awareness of control systems vulnerabilities to users and industry. There are existing mechanisms that can be adapted to support this type of activity such as Carnegie-Melon University and KEMA's activities within the CERT/CC and others.

- ***Provide sufficient funding for the National SCADA Test Bed*** to facilitate the timely and adequate determination of the actual vulnerabilities of the various control systems available in the market and develop appropriate mitigation measures.

Control Systems Design Considerations

Control systems were originally designed to be isolated. - Control systems are used throughout all industrial manufacturing, utility operations and management, transportation, and other critical infrastructure sectors. Control systems are unique in their design and are directed to perform specialized tasks. They were originally designed to be isolated - that is, separate from other corporate enterprise computing. Unfortunately from a security perspective, competitive pressures have forced businesses to interconnect office and electronic commerce systems with these control systems. This has inadvertently exposed control systems directly to the Internet, intranets, and remote dial-up capabilities that are vulnerable to cyber intrusions.

The control systems industry and its users are not well positioned to utilize security technologies as they are being developed and implemented in traditional business IT applications. - Control systems are designed with digital processors that have limited computing resources that are specifically designed, implemented, and embedded into their various process control equipment. Control systems are ubiquitous throughout many industries and are expected to have long-term use (more than 5 to 10 years) before replacement is necessitated. Unlike traditional business systems, control systems are not typically replaced when a faster, more powerful processor or new operating systems release is developed. Control systems are replaced when the system becomes obsolete, cannot be supported for lack of parts, or can no longer support functional requirements. Consequently, the control systems industry and its users are not well positioned to utilize security technologies as they are being developed and implemented in traditional business IT applications. Further, economic pressure dictates that minimal upgrade and improvement funding is available in today's competitive environment.

Control systems design constraints preclude use of existing security technology. - Control systems are deterministic in their design and operation. That means these systems have been designed with critical timing requirements, rigid performance specifications, and specific task priorities. These systems are also computer-resource and communication bandwidth limited. These constraints preclude use of existing security technology such as NIST-approved block encryption and Public Key Infrastructure (PKI). Block encryption and PKI are too resource intensive for many legacy control systems and may actually cause the systems to fail as they attempt to keep up with the intensive demands on their limited resources.

Control systems communications utilize industry-accepted protocols that were designed without security considerations. - Many installations believe that having a firewall around the control system is sufficient. Firewalls may be one part of the security solution, but firewalls can be configured to be very restrictive or configured to be open. Unfortunately, my experience has shown that firewalls for control systems are not always configured effectively. Further, they are designed to filter Internet Protocols (IP) and were not designed to filter communication protocols used for control systems communication. Attempting to filter control systems protocols will require utilization of additional protective devices that may result in either unacceptable performance delays or require that control system information must be communicated without any filtering.

Control Systems Culture Issues

What I am describing is a multi-fold cultural and technology gap that needs to be overcome. In most organizations information technology (IT) departments are responsible for cyber security. IT is traditionally well versed in cyber security for the commercial applications and have funding, although not necessarily sufficient funding to address all threats. IT also frequently reports through an organization's Chief Information Officer (CIO) to the executive board. However, IT typically does not have responsibility or accountability for the control systems that are a major component of their business and our critical infrastructure. On the other hand, an organization's operations-focused department is usually responsible for the control systems, but is typically not well versed in cyber security and often has little or no funding for cyber security.

There is often animosity between IT and operations. IT is perceived as not understanding what it means to maintain a system that has a greater than 99.99 percent reliability requirement and that must be available around the clock. As a point of illustration of this dichotomy, a two-level security solution that IT often proposes includes the requirement to add an additional password login function. This requirement might prevent a substation or power plant engineer from addressing a real-time outage or incident while attempting to get past a password lockout.

Another example of the IT-operations culture problem is that field engineering and maintenance personnel have, as their primary obligation, a duty to keep facilities operating. That obligation often translates into establishing remote dial-up or Internet connections to remotely access the control system to quickly diagnose existing problems. Unfortunately, this capability is sometimes implemented in a manner that is unknown to IT or to Central Engineering. Many of the system components share both phone lines and high-speed internal intranet connections - a significant, yet undocumented backdoor to the control systems.

Another concern is the use of non-control systems engineers to analyze the cyber vulnerabilities of control systems. Control systems have unique requirements that are uncommon and unfamiliar to the inexperienced control systems investigator. Two issues in particular are brought to mind: (1) the impact of performance on control systems when applying traditional IT security mitigation, and (2) the failure to spot significant cyber vulnerabilities that are not IP-related. The most likely way that cyber intrusions can be used to cause physical damage to equipment is not through the IP/Ethernet, but via non-wired approaches such as dial-up modems, direct connections to control networks by "foreign" laptops, and other similar means. Ideally, a team with both IT security and control systems expertise should perform control systems cyber vulnerability assessments.

Control Systems Cyber Vulnerabilities

Electric utilities often require their vendors to supply the source code for SCADA/Energy Management System (EMS) applications. Utilities are also provided detailed technical manuals, training, and default passwords for vendor remote-access. There are only a limited number of SCADA/EMS suppliers and many are U.S. subsidiaries of foreign corporations with shared development in various European countries. The same systems installed in North American control centers are installed throughout the world, including in countries not necessarily friendly to the U.S. Consequently, utilities in countries defined as "unfriendly" have a detailed understanding of the software and configuration of systems installed throughout North America.

Reliable operation of control systems depends on telecommunications including voice, data, radio, and microwave. In some cases, the telecommunications system is wholly under the ownership and operation of the utility. In other cases, telecommunication facilities are leased from telecommunication providers. These telecommunication providers have inadvertently contributed to control system unavailability (denial-of-service). For example, during the Slammer worm incident in 2003 the worm affected a telecommunication provider's frame relay network, thereby preventing communications to and from a utility's substation SCADA control system. In this case, the substation SCADA was effectively inoperable for approximately six to eight hours.

Currently, telecommunication vulnerabilities are not always addressed in control systems cyber security assessments or in programs including the NERC Cyber Security Standard-Urgent Action Standard 1200. Another example of how telecommunication vulnerabilities can impact control systems was revealed during an electric utility IT Telecom field audit of all phone lines in its operational facilities. The audit identified approximately 100 to 200 phone lines installed in power plants and substations that were not owned, or accounted for, by the utility. These phone lines were owned, installed, and paid for by the control and diagnostic systems' suppliers, because the lines required modems for remote access to the control systems to meet warranty requirements. Since the phone lines belonged to the vendor and not the utility, the phone lines did not have the utility's telephone prefix and were not identified in any war-dialing exercise. This is a common occurrence on many control system implementations throughout all critical industrial infrastructures.

Not being aware of phone lines installed in the field is one of many examples that can be cited in support of the need to benchmark the security status of facilities. This benchmarking process requires several activities:

- Performing vulnerability assessments to establish a baseline and then self-assessments to assure security is not being breached as systems are modified or changed. Detailed methodology needs to be developed.

- Performing a probabilistic risk assessment (PRA) of the vulnerability results to determine the level of mitigation required based on cost vs. risk. The PRA methodology has been used for commercial nuclear facilities, but will need to be adapted to meet control systems security applications. Additionally, training will be required for its implementation.

- Developing a detailed configuration management/configuration control program that identifies the current hardware, software, communication protocols, communication media, and patch level of control systems as-installed in the field.

- Developing detailed security policies and procedures specifically for control systems identifying activities that could compromise control systems security. This requires control systems, system operations, and IT security expertise.

Electronic vulnerabilities in operational systems are impacted by a variety of factors such as:

- Equipment suppliers provide remote dial-up access as part of their standard system configuration and utilize default passwords.

- Plant staff is reluctant to change default passwords because of personnel performance considerations during emergency events.

- Plant and corporate staff use remote desktop access software without adequate security considerations to manage and operate systems from off-site locations.

- Security patches often are not supplied to the end-users, or users are not applying the patches for fear of impacting system performance. Current practice is to apply the upgrades/patches after the PCS/SCADA vendors thoroughly test and validate patches, sometimes incurring a multiple-month delay in patch deployment.

- Most new control and diagnostic hardware and software are web-enabled or wireless, creating potential cyber vulnerabilities unless specifically addressed.

- Control systems networks utilize Internet-based control and diagnostic applications without IT Security's knowledge.

- Power marketers often feel they require immediate access to data generated by DCS and SCADA systems and often directly access these systems from the Internet to retrieve the data.

- Insecure tools such as ActiveX controls are packaged as part of the control system architecture.

- A common security recommendation for servers is to turn off or remove services that are not needed by the application (such as NETBIOS or Telnet). However, a pervasive problem with applications in general, and specifically with control systems, is that vendors do not document the services that are required for their software to properly function. They quite often install and turn on services that are not needed and use services known for their vulnerabilities when more secure alternatives are available (for example, Telnet vs. ssh-secure shell). This unnecessarily complicates the job of removing vulnerabilities and keeping systems patched and secure.

- Protocol analyzers are publicly available to translate and issue commands for control systems communication protocols making "security by obscurity" less relevant.

There have been numerous discussions and recommendations for preventing a recurrence of the August 14, 2003, Northeast Outage. In order to address reliability issues associated with the older electromechanical relays and switches, there has been a push to install new digital networked devices without necessarily addressing the newly created cyber vulnerabilities. Ergo, we are moving from a "cyber-dead" environment to a very "cyber-alive" environment that is more capable, extensible, and reliable, but also more vulnerable.

The Threat

Cyber attacks on control systems can be targeted at specific systems, subsystems, and multiple locations simultaneously from remote locations. Such attacks can directly challenge equipment design and safety limits, potentially causing system malfunctions and shutdowns. Electronic attacks also can impact restoration efforts by manipulating procedures or dynamically changing equipment conditions.

Actual Cases

Various cyber security intrusion studies by the Department of Energy and by commercial security consultants, including KEMA, have demonstrated the cyber vulnerabilities of control systems to unauthorized access. There have been more than forty real-world cases where control systems have been impacted by electronic means. These events have occurred in electric power control systems for transmission, distribution, generation (including fossil, gas turbine, and nuclear, where three plants experienced denial of service events), as well as control systems for water, oil/gas, chemicals, paper, and agri-businesses.

Some of these events have resulted in damage. Confirmed damage from cyber intrusions have included intentionally opening valves resulting in discharge of millions of liters of sewage, opening breaker switches, tampering with boiler control settings resulting in shutdown of utility boilers, shutdown of combustion turbine power plants, and shutdown of industrial facilities. However, none of these events have been identified in the traditional Internet monitoring organizations such as CERT/CC, SANS, or the Computer Security Institute-CSI. Additionally, none of the events and statistics quoted by these organizations specifically address control systems. As defined in the CERT for Control Systems (e-CERT) section below, this is a gap that needs to be addressed.

Potential Scenario

There are many "doom and gloom" scenarios. I believe most cyber impacts will be minor in nature. However, very determined, knowledgeable attackers could potentially create long-term impacts on portions of the electric grid, especially when fed by single, critical substations. In May of last year, I developed a hypothetical scenario with input from several utility and DOE National Laboratory personnel on how, using only cyber, it would be possible to impact or shut down portions the electric grid for extended periods of time (e.g., from days to months). I presented this scenario at the May 2003 Georgia Tech Protective Relay Conference. The approximately 300 utility and vendor protective relay engineers concurred it was a plausible scenario. They only questioned impact duration, concluding that impact duration was a function of local redundancy, available spares, and backup capability.

Market Issues

Control systems suppliers and diagnostic hardware and software system suppliers are responding to the market by supplying systems that are either Microsoft-based, web-based, and/or wireless enabled. Consequently, there may be inherent design and implementation of cyber vulnerabilities included in the products as delivered. Many vendors are not supplying secure control systems, perhaps because they feel there is no market for them. In addition, end-users are not specifying secure control systems in their purchase specifications since there is no mandate, nor do they want to spend the additional money it would take to develop a secure control system.

An additional issue is that there are no specifications to define a secure control system. Several groups including NIST's PCSRF and ISA's SP99 Committee are currently attempting to develop security specifications that end-users, system integrators, and control system vendors can reference.

Securing Control Systems - What is Needed

Several key activities need to be addressed and require funding to secure control systems. It should be noted that control system cyber security improvements will have direct relevance to the entire industrial manufacturing enterprise in addition to the electric power industry.

CERT for Control Systems - eCERT

I believe a primary reason why industry has been slow to respond to the issue of control system cyber security is the belief that vulnerabilities and risks are not real. I am not aware of a business case that has been developed for damage potential and associated costs. There has been almost no public identification of control systems intrusions, and therefore it has been difficult for companies to build a business case for more secure control systems.

Many groups manage and disseminate incident and vulnerability information for the Internet and other cyber-susceptible information systems. No one is providing this service for the PCS/SCADA environment on a consistent basis. As an example the CERT/CC at Carnegie-Mellon's Software Engineering Institute currently is not set up to monitor control systems intrusions or events. There is a need for industry-specific assessments and expertise to add credibility and value to the CERT process. Providing a service like a CERT for PCS/SCADA systems would have a far-ranging value and offer benefits across all utility and critical infrastructure industries.

An industry-wide CERT for Control Systems – "e-CERT" - could gather information from the various industries that use the same technology, making industry-specific Information Sharing and Analysis Centers (ISACs) more useful by providing information independent of any industry sector. Since the same PCS from vendor "X" is used in power, water, refineries, chemical plants, and paper mills, information on cyber vulnerabilities from any industry utilizing a PCS from vendor "X" would be of interest to all other industries (even if they are not considered critical infrastructures).

The e-CERT also could help dispel the various myths circulating that impede the awareness effort. I compiled one of the most comprehensive databases of control systems impacts in the power industry in an informal and unstructured manner to begin this awareness process. As a result, DOE's Office of Energy Assurance (OEA) funded KEMA and Carnegie-Melon's Software Engineering Institute (CERT/CC) to prepare a scoping study for establishing the value of an energy-related CERT, e-CERT.

There is a need for a technical organization (such as CERT/CC) trusted by industry (vendors and end-users) that can gather sanitized information and have the technical expertise to analyze this information. I believe that the e-CERT concept could be one of the most valuable services the government can provide. It is anticipated that a steering group consisting of end-users, National Laboratories, and equipment suppliers would provide guidance on requirements, benefits, and process. The intent would be to have e-CERT analyze the information, work with the National Laboratories at the various SCADA and PCS test beds to determine the impacts, and then make that information available to the appropriate industry ISACs and relevant control systems user groups. The initial annual funding level would be on the order of $3 million, which seems a small price to pay to help secure the nation's critical infrastructures and the overall industrial manufacturing base.

National SCADA Test Bed

To date, there has not been a concerted, independent effort to determine the exact vulnerabilities of control systems or the types of technology that should be employed to secure control systems. Rather, there has been an assumption that the encryption technology utilized to ensure confidentiality of data and communications over the Internet and traditional IT business systems will be sufficient for control systems. However, for control systems, confidentiality is not the primary security objective. For control systems, availability and message integrity are most critical, whereas confidentiality is secondary.

Most vulnerability assessments and intrusion testing of control systems in actual operation stop short of actually attempting to gain unauthorized access to the control systems. This is because the risk of interfering with the processes these systems control is too great.

Consequently, two critical areas need to be addressed to better secure control systems:

- Understand the damage that can be done if a control system is compromised, and

- Develop security technology specific to control systems that improves security without impacting the performance requirements.

The National SCADA Test Bed is in a unique position to meet these requirements. The Test Bed combines the best skills of the Idaho National Engineering and Environmental Laboratory (INEEL) and the Sandia National Laboratory (SNL) working together to secure critical infrastructure.

The large scale Test Bed is located at INEEL. INEEL has its own 138,000-volt grid independent of the local utility. This enables the Test Bed to test equipment in a representative environment. It also provides the capability to determine not only if a potential intruder can "touch" the control system and gain unauthorized access, but also determine what damage can be done to the control system and the grid it is monitoring and controlling. The National SCADA Test Bed can, therefore, determine what mitigation technology needs to be developed. Additionally, the vulnerability assessments will be used as a starting point to develop security technologies specifically for control systems.

To date, several SCADA and other control systems vendors have provided control systems to the Test Bed. The National SCADA Test Bed is vendor independent and trusted by vendors and end-users. Consequently, the information from the Test Bed will be trusted by the industry, will allow off-line testing and validation of processes and procedures, will improve industry awareness, and will enable rapid dissemination of critical information (such as through e-CERT).

Another key function of the Test Bed will be its interaction with e-CERT. e-CERT, through its trusted relationships, could be the direct interface to industry in collecting and sorting vulnerability information and then performing preliminary assessments. That information will be supplied to the Test Bed for use in field-testing of actual control systems to confirm vulnerabilities and potential impacts. The Test Bed will then determine potential mitigation technology (hardware and/or guidelines) that can be disseminated through e-CERT, ISACs, and other avenues to the appropriate organizations.

Adequate funding is lacking to enable the Test Bed to function in a complete and timely manner. A significant multi-year investment is required.

Summary/Conclusion

Control systems are different from traditional IT systems. The technology and information sharing necessary to secure these systems are not currently available. e-CERT and the National SCADA Test Bed can help strengthen the security of the control systems that are an integral part of the nation's critical infrastructure. A secondary benefit would be improved reliability and availability of the critical infrastructure services.

I am concerned that if we do not take these and more actions, the reliability and availability of our critical infrastructure will be vulnerable to intentional, or even unintentional, events in ways we have not contemplated.

Thank you Mr. Chairman, Committee Members, for your time and attention. I am happy to answer questions.

###

Joseph M. Weiss, P.E., C.I.S.M., is an Executive Consultant with KEMA Inc where he serves as a leading industry expert on control systems cyber security. He can be reached at jweiss@kemaconsulting.com.

KEMA Inc. is based in Burlington, Massachusetts with approximately 400 technical and management consulting specialists in offices throughout the United States and abroad. Assisting over 500 clients in more than 70 countries, KEMA provides technical and management consulting, testing, inspections, certification, and training services to utility and other process industries and end-users. More information on KEMA, Inc. can be found at www.kemainc.com.

Mr. PUTNAM. Thank you, Mr. Weiss. You will undoubtedly get some questions on that.

Our next witness is Dan Verton. Mr. Verton is a senior writer and investigative reporter with ComputerWold Magazine based in Washington, DC, where he covers homeland security, critical infrastructure protection, and Government. Prior to joining ComputerWorld, Mr. Verton was the associate editor for defense at Federal Computer Week. He entered the journalism field after 7 years in the military intelligence community as an intelligence officer in the U.S. Marine Corps. He has a master's degree in journalism from American University in Washington.

You are recognized for 5 minutes. Welcome to the subcommittee.

Mr. VERTON. Thank you, Mr. Chairman. In the interest of time, obviously, I am going to summarize my remarks today, but actually I am going to diverge a little bit from what I had planned to say based on what I have already heard from the previous panel. I think what I have heard so far has been quite instructive for your work in this area.

This hearing is supposed to be about SCADA systems security and telecommunications. But, surprisingly, what I heard from the first panel was that we are, in fact, at this current time erecting fences and digging moats around physical facilities that house SCADA systems. So where does this disconnect come from? I have a feeling it comes from the one individual from the Government that I do not see here that I think you would very much benefit from hearing from, which is Amit Yoran. I sat behind Mr. Yoran a few weeks ago in the Senate and listened as we were discussing the National Intelligence Estimate that was recently released or was supposed to have been released on the cyber threat to the United States stemming from, specifically, terrorist organizations around the world. And I was a little bit surprised that our director of national cyber security could not answer any general questions about the terrorist threat to the United States in the cyber realm.

So I do not think it is necessarily doing anything for us to be creating layered defense in depth in a physical sense when the electronic infrastructure that powers these systems knows no borders. This also I think stems from what I think is a very dangerous approach to countering terrorism in cyberspace, which is the threat independent model. DHS takes a threat independent approach to threats in cyberspace. And what does that mean? That means that we approach terrorist incidents the same way we might approach a hurricane or a flood or an earthquake. And I think the danger that lies in this is that it presents us with a possibility of having the lowest common denominator for security when in fact you are talking about, for example, a hurricane which is very indiscriminate and random, whereas terrorist incidents are very much a highly targeted, very specific incident that might be indiscriminate in the killing and destruction, but it is very much a highly, well-planned incident that we are talking about. And I think we need to take that into consideration when we talk about these critical facilities.

Finally, just briefly, I think there is some questions that should be asked about the funding for cyber security in the grant process. We were talking in the first panel about the money that has been made available to the States and localities. But I think there has been some questions raised out there about how that money can be used. So while the money may be used to build fences and dig moats around these facilities, I think there is some question out there about how much of it, if any of it, can be used to fund cyber security improvements for the SCADA systems.

Basically, I think our challenge today stems from two perspectives. I think we need to try to reverse the intellectual rigidity that surrounds the issues of cyber terrorism. We already knew from evidence prior to August 14th that Al Qaeda had been studying SCADA systems from some of the evidence that we had picked up on the battlefield in the war on terrorism. If there was any doubt in the minds of the terrorists who are also trying to kill us that they should be studying SCADA systems, the international demonstration effective August 14th pretty much eliminated that doubt in their minds.

Second, I think if we insist on continuing to refer to these facilities, as we have here today, as critical to national security, we should treat them as such. I am aware of anecdotal evidence from people who are very much involved on the inside of the energy industry that not all people with authorized access to critical control systems are necessarily subjected to background investigations, and this is across the board, it is not just the energy industry. These are individuals with authorized access to the systems that both touch SCADA systems and to SCADA systems themselves. That is a vastly different picture from any national security infrastructure that I have been aware of in my time as an intelligence officer.

And just one final point on the Web content, which you were asking about earlier. I wrote an entire book on the fact that the information we make available to the people who are trying to do us harm is really, as was mentioned, beyond the pale. It is unbelievable what you can find on the Internet. Now the genie may be out of the bottle already. But let me give you an example of just what I was able to dig up during my research.

There are Web sites that provide interactive maps of the entire natural gas pipeline system in the United States. And they are not flat files. They give you latitude and longitude for every critical interconnection point in the United States, including the most critical interconnection point for the natural gas industry in the country. Some 40-plus percent of the entire GDP of natural gas passes through this one interconnection point. And you can not only find the latitude and longitude, but you can find the terrain features surrounding the particular point. And you can do this for the entire United States. I found that on the Internet during my research, including long-haul telecommunications termination points along the entire Eastern Seaboard, so on and so forth. So I think there is an argument to be made for a public policy approach to what we provide on the Internet, who we provide it to, and whether or not there is a business case for any of this information being out there.

So with that, Mr. Chairman, I will be happy to answer any questions.

[The prepared statement of Mr. Verton follows:]

March 30, 2004

Statement for the Record of
Dan Verton
Senior Writer, Computerworld Magazine
Author, Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw-Hill/Osborne, 2003)

On

Security and Telecommunications of Industrial Control Systems in our Nation's Critical Infrastructure

Before the
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
House of Representatives Committee on Government Reform
Washington, D.C.

Good afternoon Chairman Putnam, Ranking Member Clay and Members of the Subcommittee.

I want to thank you and your staff for the honor of appearing before you today to discuss what I believe is an urgent national security matter and I applaud your leadership in this area.

At the outset, let me say that I appear before you today as somebody with no vested corporate interest in the outcome of this hearing and as an independent researcher whose statement and answers stem from years of confidential discussions with well-informed sources in the national security arena. Although I do not consider myself a technical expert in the control systems used in many of our nation's most critical industrial settings, I have a professional background in intelligence and information security, and I'm the author of a newly published book by McGraw-Hill titled *Black Ice: The Invisible Threat of Cyber-Terrorism* that goes into detail regarding the subject of today's hearing and that has been endorsed by some of the nation's leading authorities in critical infrastructure protection, terrorism and information security, including the president's two former chief cyber security advisors, Richard Clarke and Howard Schmidt.

Supervisory Control and Data Acquisition systems, or SCADA systems, are in many ways the crown jewels of some of the nation's most important industrial control settings, such as the electric power grid. But they are not – as their name might imply – built upon secret, proprietary technology. To the contrary, modern design specifications for SCADA systems, which I have documented through both personal interviews with experts and through open-source research on the Internet, presents us with the frightening reality that the SCADA systems being used in our nation's critical infrastructures are nothing more than high-end commercial PCs and Servers running Microsoft Corp. operating systems. In other words, the genie is out of the bottle and has been for years in terms of understanding how to disrupt or corrupt the operations of SCADA systems. Today, it's simply a matter of gaining access. And as I have also documented in my research, gaining access to SCADA systems for the purpose of causing widespread chaos, confusion and economic damage is increasingly becoming a mere formality for professional hackers, virus and worm writers, and terrorist-sponsored saboteurs.

However, before I get to the critical issue of open access to SCADA systems and the vulnerability that they now increasingly face, let me say a brief word about the critical national security implications of this growing problem. Despite the impact of the Slammer worm and possibly the Blaster worm on the electric power industry – a primary user of SCADA systems for management and control of the electric grid -- the problem facing us today extends far beyond the electric power industry. While the electric power grid can be considered the first Domino in a cascading failure of critical infrastructures, SCADA systems are critical to the day-to-day and minute-to-minute operation of the natural gas pipeline system, chemical processing facilities, telecommunications networks, as well as municipal water and wastewater systems to name just a few. And while all of these sectors differ in terms of their level of modernization, all share a common modernization approach, which is based primarily around Web-based and wireless technologies for cost-savings and ease of management. And that brings me back to the issue of access to SCADA systems and their potential vulnerability.

We know for a fact that the forces of deregulation have given rise to an increasing number of deliberate and inadvertent connections between SCADA systems in the electric industry and the Internet-based corporate networks that utilities use to manage the business of buying and selling power. In fact, the integration and interoperability of SCADA systems with corporate IT systems is, in some cases, institutionalized as part of the IT contracting and acquisition process at some utility companies. For example, companies often require SCADA systems to be interoperable with corporate architectures (e.g., must be Windows 2000 and use the following password and logon structure . . .) before the systems can be purchased. All of these connections provide avenues of attack for hackers and terrorists online and also expand the universe of the so-called "trusted insider." All of this is of particular concern when you factor in statistics that indicate the average large utility company deals with about 1 million cyber security incidents per year that require some sort of investigation or response.

The energy industry has acknowledged the existence of these linkages and the imperative of protecting SCADA systems from unauthorized access. In December 2001, for example, the American Gas Association and the Gas Technology Institute met in Washington, D.C., to discuss the need for improved encryption to protect SCADA communications between key nodes in the natural gas grid. One of the slides used during the two days of presentations highlights the threats posed to SCADA communications from the use of commercial computer equipment, open communication protocols that are widely published and available to anybody, linkages and reliance on the public switched telephone network, and the ability to steal the hardware.

In addition, a recent network architecture plan released by a major company in the water and wastewater industry included the following requirements for its SCADA systems: Peer-to-peer networking over TCP/IP (Transmission Control Protocol/ Internet Protocol—in other words, the Internet); software changes that can be downloaded from any node on the network; dial-in capabilities to all software functions; and a link to the existing pump station.

Consider the following additional examples, which I document in my book, Black Ice; The Invisible Threat of Cyber-Terrorism:

The U.S. railroad system's increasing use of wireless technologies may present one of the most immediate dangers to both national security and local safety. Given the system's long, winding network of radio, telephone, and computer assets, voice and data communications networks provide vital links between train crews, trackside monitoring and repair staff, and rail control centers. Total control of the massive network is accomplished through a communication system that integrates trackside maintenance telephones, trackside transponders, security cameras and monitors, passenger information displays, public announcements, the public telephone network, radio bases, and control center consoles. However, wireless SCADA systems are increasingly providing the management glue that keeps all of these systems running together. In the colder regions of the country, underground heaters keep the rails from freezing in winter. These operations are also being controlled and monitored by wireless SCADA computers. The use of modern technology in this case means that in the case of a failure, railroads no longer have to dispatch technicians in the dead of winter to remote locations where heating switches are usually located. However, it also means that the security of these switching operations may now have a new series of security challenges to deal with. This is of particular concern given the dangerous nature of some train cargo.

The City of Brighton, Michigan, is one example. Brighton is a city of only 6,500. But that population skyrockets to more than 70,000 each day due to a thriving business district and a boom in hotel space. However, beneath the streets of Brighton is a **water and wastewater system** that is controlled in part by wireless technology. The remote terminals monitor pump run time, pump failures, flood sensors, high water level alarms, and power, as well as site intrusion alarms and manually activated panic buttons. The utility also planned to equip work vehicles with a controller connected to a laptop computer. "With critical data now available at just the click of a mouse, the laborious, time-consuming, and often hazardous, need for utility workers to make daily rounds to check pump status at each of the lift stations is a thing of the past," claimed marketing material from one of the contractors responsible for installing the equipment. The mobile controller would then allow utility engineers to monitor the waste water system while they're driving around the city.

Uranium mining operations in Wyoming extract uranium from the soil through a process by which water is injected into the ground. Because of the contamination, remote terminals are necessary to control and manage the pumps that move the water and extract the uranium. Commercial PC-based remote workstations now support critical monitoring functions, such as pump failure, pump status, temperature, speed, and even the pump's on/off condition. But the security implications are enormous. When pumps lose power, water pressure starts building up in the plant. Software has been programmed to automatically reset certain pumps to get the pressure out as fast as possible. And it's all being done in the name of cost-effectiveness.

In states throughout the **Midwest, one can find oil wells** arranged in a twelve-mile-diameter circle. They are part of what's known in the vernacular of the oil industry as a **"water flood" operation**. However, with such a large number of pumps and holding tanks to manage, drilling companies are increasingly turning their attention to wireless SCADA systems to monitor critical functions of the operation, including emergency systems that are designed to ensure environmental safety. For example, wireless SCADA systems are used to monitor pressure and flow rates in both oil and water pipelines. When flow rates drop below normal levels, the system is designed to turn on additional pumps. In addition, if pipeline pressure or tank levels exceed normal operating limits the system will turn various pumps off. They are also used to monitor tank levels and overflow pit levels —a critical safety indicator that could have environmental consequences if it fails. And as in the case of the 911 emergency systems, oil well managers and technicians also have remote dial-in connection capabilities.

Mr. Chairman, let me conclude with a final word about how we must think about these vulnerabilities in post-Sept. 11 America.

The pervasive intellectual rigidity that surrounds the issue of cyber-terrorism has created two competing camps of thought. One camp, consisting mostly of individuals with years of formal training and experience in national security from a holistic point of view (i.e., the relationship between physical security and cybersecurity, and the adaptive nature of international terrorism), accepts the notion that America is facing a thinking enemy that is far more capable than most people are willing to accept. The other camp, consisting mainly of self-proclaimed experts, industry "analysts," and Internet security professionals whose expertise is limited significantly to the virtual realm of the computer, remains the last, fading bastion of hope for those who want desperately to hang on to the conception of traditional "physical" terrorism as the only legitimate form of terrorism. This latter group falls into the same category as those who, prior to September 11, 2001, considered airborne threats to physical infrastructure too bizarre to spend time and resources preparing for.

Since the start of the U.S. War on Terrorism, a significant amount of evidence has been unearthed throughout Afghanistan and various other al-Qaeda hideouts around the world that indicates terrorism may be evolving toward a more high-tech future at a faster rate than previously believed. In January 2002, for example, U.S. forces in Kabul discovered a computer at an al-Qaeda office that contained models of a dam, made with structural architecture and engineering software. The software would have enabled al-Qaeda to study the best way to attack the dam and to simulate the dam's catastrophic failure. In addition, al-Qaeda operatives apprehended around the world acknowledged receiving training in how to attack key infrastructures. Among the data terrorists were studying was information on SCADA systems.

For the most part, these dire warnings have gone unheeded by the private- sector companies that own and operate these infrastructure systems. Senior executives view such scenarios as something akin to a Hollywood movie script. However, throughout the entire post-September 11 security review process, a process that continues to this day, administration experts and other senior members of the U.S. intelligence community were quietly coming to the conclusion that they were witnessing the birth of a new era of terrorism. Cyberspace, with its vast invisible linkages and critical role in keeping America's vital infrastructures and economy functioning, was fast becoming a primary target and a weapon of terror.

Mr. Chairman, my fear is that the next time we have a massive power failure, such as we experienced on Aug. 14, it will not be a self-inflicted wound, but potentially a terrorist-induced failure that is quickly exploited by suicide bombings, rampaging gunmen or chemical and biological attacks against those stranded in the subway systems. Real-world, cross-border exercises between the U.S. and Canada, including one from which the title of my book is taken, have already shown that physical and cyber attacks can cause cascading failures throughout multiple regional infrastructures, including power outages that could last for several months. And these exercises were written and war-gamed by the actual owners and operators of critical infrastructures based on a self-assessment of their own worst fears and worst-case scenarios. After action reports indicate that infrastructure owners have at best a surface-level understanding of the interdependent nature of their infrastructures and few know exactly how to prevent such failures from spreading out of control.

My recommendations to the Subcommittee are as follows:

1. Require background investigations or security clearances for private sector workers with direct access to SCADA systems, control centers or communications facilities that operate our nation's most critical infrastructures. This is a national security issue and it should be treated as such.
2. Red Team the infrastructure immediately and independently. It is time for "Eligible Receiver II." The government should develop, sponsor and conduct a "no-notice" Red Team assessment of the nation's critical infrastructures to determine the true level of security and preparedness.
3. Push the "market" into action, because the market will not and has not volunteered to be the defender of America in this age of Internet-enabled threats. This will require a mix of new regulations coupled with insurance industry action to offer premiums that are responsive to government-certified security audits. This is not heavy-handed government regulation, it is leadership in the form of "Trust, but verify."
4. Sponsor a more aggressive research & development program in SCADA system security devices and software. The genie is out of the bottle. The international demonstration effect of Aug. 14 cannot be denied.
5. Congress should provide strict oversight of the energy industry's $100 billion upgrade program for the next generation power grid to ensure that security is the first priority. Separate networks, similar to the failed GovNet initiative, should not be taken off the table.

I thank you for this opportunity to share with you some of my research and opinions on this matter. I would be happy to answer your questions.

Additional Resources:

Blaster Worm Linked to Severity of Blackout
http://www.computerworld.com/databasetopics/data/story/0,10801,84519,00.html

CIOs, Experts Cite Urgent Need for U.S. Infrastructure Upgrade
Some energy CIOs and experts said similar or worse failures are possible in the future if the industry and government fails to develop more modern control systems.
http://www.computerworld.com/industrytopics/energy/story/0,10801,84096,00.html

Black Ice
In his new book, Black Ice, Computerworld's Dan Verton says the private sector is in a state of denial about the serious threat of cyber-terrorism against power plants, telecom sites and other critical facilities.
http://www.computerworld.com/industrytopics/energy/story/0,10801,83841,00.html

Utility Companies Face Barrage of Cyberattacks
Many utility companies, which own and operate critical power networks, are finding it more and more difficult to keep up with the number of cybersecurity incidents involving their control systems, according to experts who attended a conference last week in New Orleans.
http://www.computerworld.com/industrytopics/energy/story/0,10801,67581,00.html

Movement afoot to beef up industrial cybersecurity
Efforts to boost IT security for major industrial-control systems that are critical to infrastructure protection are picking up steam.
http://www.computerworld.com/industrytopics/energy/story/0,10801,70587,00.html

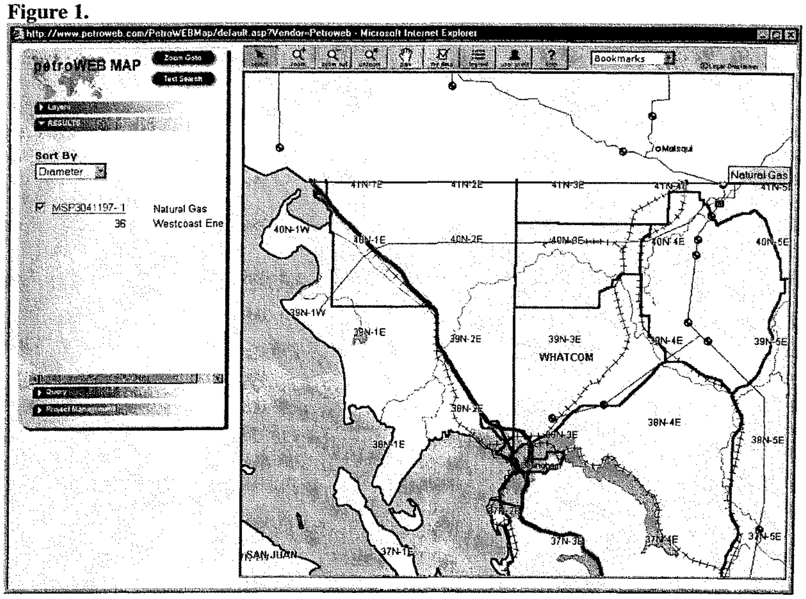
California Hack Points to Possible Surveillance Threat
The revelation that hackers broke into computer systems owned by California's primary electric power grid operator and remained undetected for 17 days this spring highlights a growing fear on the part of federal officials that such intrusions could be part of long-term intelligence-gathering activities.
http://www.computerworld.com/industrytopics/energy/story/0,10801,61432,00.html

Sept. 11 lessons drive key aspects of Bush cyberdefense plan
Physical security, industrial control systems and tests of federal IT security are all featured prominently in the national strategy unveiled yesterday.
http://www.computerworld.com/governmenttopics/government/story/0,10801,74359,00.html

Energy: The First Domino in Critical Infrastructure
More research and development is needed to protect critical industrial systems in the energy sector against cyberattack, officials say.
http://www.computerworld.com/securitytopics/security/story/0,10801,74077,00.html

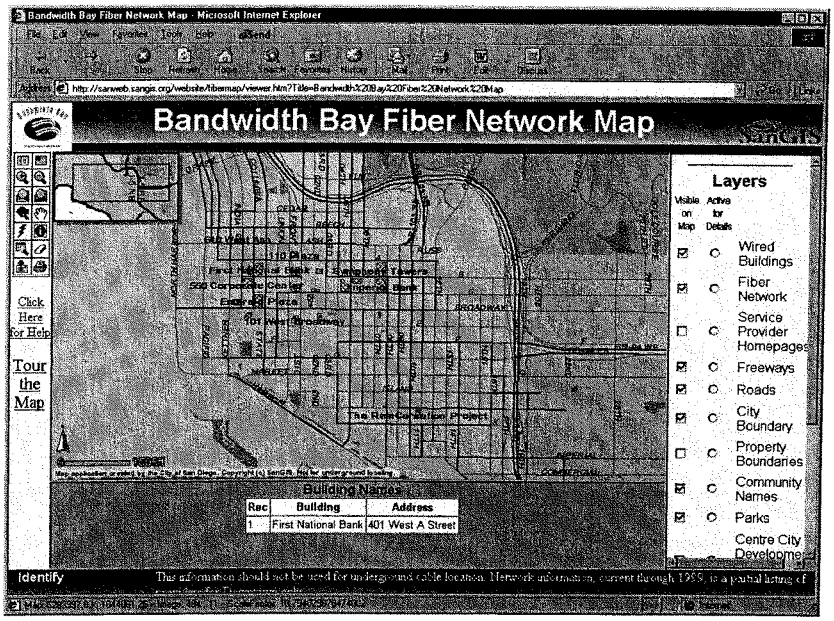
The Genie Is Out of the Bottle

Figure 1.



This is a photo taken from a publicly available Web site that depicts the most sensitive natural gas pipeline interconnection point in the U.S. What's interesting about this Web page is that it is completely interactive, not only allowing the user to zoom into great detail, but also providing latitude and longitude coordinates and detailed terrain/man-made landmarks.

Figure 2



Building Names

Rec	Building	Address
1	First National Bank	401 West A Street

This information should not be used for underground cable location. Network information, current through 1999, is a partial listing of

Detailed, street-level maps of metropolitan area fiber networks are also available online, and include building and company names through which these high-speed interconnections pass.

Other Sensitive Data Available on Government & Corporate Web Sites

1. Detailed maps depicting the termination points along the entire Eastern Seaboard for all long-haul undersea fiber lines.
2. Maps depicting the storage locations of all spent nuclear fuel waste in the U.S.
3. Telecommunications network maps from which the location of current and planned critical facilities and nodes can be derived.
4. One telecom company offered location information for all of the company's five data centers, as well as a virtual tour inside a "typical" center, including a description of all security systems used to protect the facility.
5. Detailed descriptions by IT companies of deployment case studies involving SCADA systems.
6. Load-bearing capacities of elevators in large office buildings as well as location of ventilation and air conditioning systems.
7. Number of people employed at certain office buildings as well as maps and interactive photos of building and facility layout.

Mr. PUTNAM. Thank you very much.

Our next witness is Gerald Freese. Mr. Freese is the director of enterprise information security at American Electric Power. In this capacity, he is responsible for defining, developing, and executing all information security programs to effectively protect AEP data and systems. He is responsible for regulatory compliance and critical infrastructure protection for cyber security, and has been instrumental in the development of the NERC cyber security standards for the energy industry. He is a recognized security and infrastructure protection expert. He is American Electric Power's primary data security architect.

You are recognized for 5 minutes. Welcome to the subcommittee.

Mr. FREESE. Good afternoon, Chairman Putnam, and members of the subcommittee. Thank you for offering me the opportunity to speak with you today. I am testifying as a representative of American Electric Power, as the director of enterprise information security of one of the largest utilities in the United States with over 11 States of operation and 5 million customers. Today I will be discussing issues of supervisory control and data acquisition, telecom interdependencies, and critical infrastructure protection.

Energy utilities use a number of communications media to connect various SCADA system components, from private microwave to fiber networks and public networks. Each of these transport methods enables the data flow to and from SCADA networks and also creates the potential pathways of attacks. In telecom network interface roles, there are a number of device exploits of instances of malicious code that can effectively disable SCADA information flow. The point to take away from this is basically that SCADA and telecom vulnerabilities are not mutually exclusive.

The growth of open systems is compounding the SCADA/telecom vulnerability issue. By use of common technology sets, public telecom providers are increasing the susceptibility of SCADA and telecom resources to multiple attacks from anywhere in the world. The open systems, with lower cost, ease of use, provide attackers with the same benefits as legitimate users enjoy. While we cannot effectively halt the move toward open system, we can work to establish best practices in security to counteract potential exploitation.

Availability of engineering and data system expertise is another factor. In Pakistan, American energy companies and vendors helped design the Pakistani infrastructure based on the U.S. model. In Afghanistan, analysis of recovered computers, as Mr. Verton mentioned, show that terrorists were engaged in research on software and programming instructions for distributed control and SCADA systems. This and the vast amount of data on energy SCADA and telecommunications available through open sources, such as the electric industry publications, FERC filings, and on the Internet strongly support the assumption that there are few, if any, SCADA or telecom system unknowns and no boundaries on accessibility to the information. The growth of open systems technology and increasing ranks of the computer skilled show us that there is no logical basis for discounting the possibility of cyber attacks against targeted telecommunications and SCADA systems or components.

The U.S.-Canadian task force investigation following the August 14, 2003 blackout concluded in its interim report that the outage across a large portion of the United States and Canada was not caused by malicious cyber events. If we substitute some well-known forms of intentional attack as the cause of the initial line malfunction, we can see that many forms of internal or external intrusion could bring the same net result. If we take that concept one step further, coordinated attacks against multiple vulnerable systems and networks over the Internet and other telecom resources could redirect processes, manipulate data and equipment, and eventually disrupt service across entire regions.

The foundation of critical infrastructure protection lies, first of all, in awareness that it is a responsibility across both private and Government domains. It must be a priority in industry backed by executive support and viewed as an incentive to investment, not a roadblock. For example, at AEP security implementation is listed in the third paragraph of the annual report, which is quite an accomplishment. Industry, with government support, must take the lead in information sharing. This is one of the critical aspects of critical infrastructure protection.

To that end, there must be a greater protection of information from public disclosure. The ISACs, the Information Sharing and Analysis Centers, through public and private collaboration, must work toward consolidating information on risk-based vulnerability assessments and remediation and extending security best practices across all critical infrastructure sectors. Cost recovery initiatives with similar information protection must be supported at the State level with the possibility of Federal tax incentives for industry to defray the significant cost of current and future security. All of these activities will provide the necessary backdrop for the diverse U.S. critical infrastructure to comply with voluntary industry standards and eliminate the need for Federal regulation.

Mr. Chairman, that concludes my statement. I would be happy to answer any questions.

[The prepared statement of Mr. Freese follows:]

The U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations
and the Census

Hearing on Telecommunications and SCADA:
Secure links or Open Portals to the Security of the Nation's
Critical Infrastructure?

March 30, 2004

Statement Submitted for the Record
By
Gerald S. Freese, Director of Information Security
American Electric Power

THE INTERDEPENDENCIES BETWEEN SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS and TELECOMMUNICATIONS FUNCTIONS IN THE ENERGY INDUSTRY

Introduction

Critical Infrastructure is built and operates on a framework of critical interdependencies. The energy industry, which either enables or supports every other critical infrastructure entity, is equally reliant on several of those same entities for its own viability. This statement will center on critical infrastructure protection as an "inclusive" concept – in this instance focusing on the interdependencies between energy Supervisory Control and Data Acquisition (SCADA) systems and the Telecommunications functions that support them. SCADA and Telecommunications are two areas where we must integrate cross-sector functional strategies into current and future infrastructure protection initiatives.

Functions of SCADA in Relation to Telecommunications Systems

SCADA is the "nervous system" of the power grid. It controls and coordinates multiple geographically separated, complex operational functions in power generation, transmission and distribution. It also concurrently monitors this operational environment by acquiring and processing vital electronic and physical system data. Telecommunications represents the intricate network of nerve pathways that connects these operational assets, providing the means by which to deliver the control instructions and update system status. These updates occur every .5 to 2 seconds from every Remote Terminal Unit (RTU) engaged in the transmission and distribution of power. The data rely on the telecommunications infrastructure to ensure their uninterrupted transfer to Control Centers that analyze the data. These updates, through operator interface or automated commands associated with 140 individual control centers together maintain the balanced flow of electricity across the three interconnects that comprise the North American grid. Without these telecommunications pathways, the SCADA "nervous system" is isolated from essential information exchange and effectively ceases to function.

SCADA and Telecommunications Vulnerabilities Not Mutually Exclusive

Energy utilities use a number of communications media to connect various SCADA system components. This array of private microwave and fiber networks, wireless radio and increasingly the public networks are all inextricably tied to SCADA operations and are either potential pathways of attacks, the ultimate victims of attacks or both. This array of private microwave and fiber networks, wireless radio and public networks, including cellular are all inextricably tied to SCADA operations and are either potential pathways of attacks, the ultimate victims of attacks or both. We have to keep in mind that Telecommunications is vulnerable in its role as a transport medium. It is subject to attacks such as "man in the middle," where transmissions are intercepted and altered, redirected or destroyed. Also, many power plants and substations use modems, vulnerable to a number of intrusion exploits, to manage equipment such as breakers, relays and switches over telephone lines. Telecommunications is also vulnerable in its network interface role, where telecom device exploits or network malicious code can create denial of service or buffer overflow conditions, effectively disabling operational data exchange with critical SCADA components. The key point is that SCADA and Telecommunications vulnerabilities are not mutually exclusive. The impact of successful exploits cuts across the "inclusive" interdependency model.

Compounding the SCADA/Telecommunications vulnerability issue is the move toward a centralized, more "open system" model with distributed computing and communications environments. This model is moving away from less vulnerable mainframe technology and private communications networks in favor of common technology sets and public telecom providers. These factors increase susceptibility of SCADA and Telecommunications resources to multiple electronic attack vectors from virtually anywhere in the world. In addition, this move to standardized, common technology enables a parallel and proportionate growth in an attacker's knowledge base and significantly increases control system and communications exploitability. Ultimately routine attacks designed to impact targets as common as all Internet connected computers will have a greater likelihood of disrupting critical SCADA communication paths.

Critical SCADA and Telecommunications infrastructures are "open books"

There is no mystery or obscurity associated with SCADA communications, configurations or protocols. One example that supports that premise centers on infrastructure development in Pakistan. SCADA and supporting telecom infrastructures there closely parallel the U.S. model. This is because their systems were designed and built with assistance of U.S. energy companies, using much of the same open technology, obtained through many of the same vendors. Also, analysis of computers recovered in Afghanistan showed that terrorists were engaged in research on software and programming instructions for distributed control and SCADA systems. These examples plus the vast amount of data on energy SCADA and Telecommunications available through open sources such as electric industry publications, FERC filings and on the Internet strongly support the assumption that there are few if any SCADA or Telecom system unknowns and no geographic constraints on specific knowledge factors. Add the growing ubiquity of common open systems technology and the increasing ranks of the computer-skilled to the equation and it is clear there is no logical basis for discounting the possibility of cyber attacks against targeted telecommunications and SCADA systems or components.

Electronic attacks against the energy and telecommunications infrastructures are less a question of "Can it be done?" than "How will it be done, to what extent, and what are the expected impacts?" The U.S. Canadian Task Force investigation following the August 14, 2003 blackout concluded in its interim report that the outage across a large portion of the U.S. and Canada was not caused by malicious cyber events. Notwithstanding that finding, if we review the interim report and substitute some well-known forms of intentional attack as the cause of the initial line malfunction, we can see that an internal or external intrusion could result in the same net result. An attack via the network, access through an unprotected modem into a data concentrator, remote access software vulnerability exploits or even a wireless network based intrusion could have resulted in a similar, and in these scenarios, hostile blackout condition. A successful undetected and coordinated attack against multiple vulnerable systems and networks over the Internet or through the phone systems could redirect processes, manipulate data and equipment and eventually disrupt service across entire regions.

Factors Contributing to Vulnerability of SCADA

In a number of companies, SCADA networks are not properly segmented from corporate networks. In others, access controls, firewall protection and intrusion detection are inadequately deployed. These factors increase their vulnerability to either incidental or directed malicious code attacks via the Internet, third parties or remote connections. Once malicious code enters the SCADA network, propagation methods can effectively initiate denial of service attacks against communications interfaces and disable control communications. In all of these instances, telecommunications is at once the enabler and the target of these disruptive attacks, but only to the extent that it is operating without the benefit of appropriate and effective protective measures.

Conclusion

SCADA systems and Telecommunications provide critical services and are inseparable in their functional roles throughout the U.S. critical infrastructure. Their continued effectiveness and their joint improvement and evolution depend on CI organizations taking responsibility for securing these networks and systems – decreasing the numbers of vulnerabilities, increasing reliability and protecting the infrastructure that provides essential services to the country.

American Electric Power appreciates the opportunity to provide this information to the Subcommittee. We would be pleased to provide any additional information the Subcommittee may require for its deliberations.

Mr. PUTNAM. Thank you, Mr. Freese.

Our fourth, and final, witness for the second panel is Jeffrey Katz. Mr. Katz is the enterprise IT consultant for PSEG Services Corp., a subsidiary of Public Service Enterprise Group, Inc., in Newark, NJ, which, among other things, serves 77 percent of New Jersey's population and is the State's largest utility. Mr. Katz has held a number of management positions within PSEG and PSEG Services Corp. in his 34 years with the companies. For the last 7, Mr. Katz has concentrated exclusively on wireless telecommunications projects and systems. Mr. Katz is also the former two-term mayor of his community.

Welcome to the subcommittee. You are recognized for 5 minutes.

Mr. KATZ. Thank you, Mr. Chairman, and members of the committee. I am here today testifying on behalf of the United Telecom Council as the Chair of its Public Policy Division. I will discuss the impact of Federal and State policies on critical infrastructures [CI] SCADA systems. UTC is the association that represents the telecom interests of America's CI entities. UTC and its association partners represent virtually every electric, gas, and water utility, and every communications network used to operate, control, and maintain our Nation's critical infrastructure.

Today our Nation depends upon reliable and available services provided by CI SCADA supported systems. They are critical and essential to the health, safety, and welfare of our Nation and our people. Just as our Nation depends upon CI services, every CI entity depends upon telecommunication systems for SCADA, telemetry, command and control, remote actuation, and protective relaying operations. In addition, for both routine communications and during disasters and outages, CI entities depend upon private internal data and voice networks to direct the work force and to restore service.

From a broad policy perspective, we ask the committee and Congress to consider this question. What Federal or State policies, laws, or regulations impact negatively upon CI's ability to avoid service interruptions, to reduce their duration and scope, and to make CI, including SCADA systems, less vulnerable to attack by non-physical intrusion? For a detailed discussion on that issue, I would refer the committee to my written testimony. However, in a nutshell, UTC asks the committee to consider these five points.

First, public access to sensitive radio frequency data provides information useful to those who would do us harm. The Federal system of record, the FCC's universal licensing system, is available to the general public through the Internet. Wireless CI, SCADA, telemetry, command and control, voice and data systems can be compromised using information contained within the FCC's public data bases. This information must be made less public, either through creation of a confidential licensing category, or by providing the FCC with other authorities, such as that enjoyed by NTIA, to make confidential certain CI spectrum use data. UTC also encourages providing NTIA with authority to share spectrum with non-Federal CI entities to assure greater confidentiality of spectrum use data.

Second, CI data is made public unnecessarily through the FCC's pole attachment regulations with little regard to infrastructure safety. Pursuant to FCC rules, maps of utility infrastructure must be made available to potential attachers upon the most minimal of showings. Moreover, those who would attach fiber optic cable or other equipment to utility infrastructure are permitted to employ third party contractors rather than personnel trained to observe strict safety regulations. The FCC's original limited jurisdiction over utility infrastructure is being stretched to the point of endangering worker and public safety. That authority should be balanced by safety-based jurisdiction elsewhere in the Federal Government.

Third, CI investment to improve and better secure communications systems is discouraged because such investments often are not immediately recoverable in rates and because the spectrum in which SCADA systems operate is not exclusive. Regulated entities recover capital investment costs through rate relief. Rate cases are time consuming, tedious, costly, and must be filed in each State in which the utility serves customers. However, most utilities have a multistate presence that would require consistent cost recovery schemes between and among the States involved.

SCADA systems are system-wide and not limited to the borders of a single State. Prudent and necessary investments in enhanced security, reliability, and functionality should be recoverable immediately in rates, without the need to file a rate case in each State, and the specifics of the investment should be privileged and confidential. Furthermore, the investment must be protected. CI entities are reluctant to invest in new wireless SCADA systems because the spectrum is not exclusive. This subjects SCADA systems to interference that can compromise effectiveness.

Fourth, State and local governments should receive guidance from the Federal Government as to what security expenditures and investments should be considered reasonable. UTC does not advocate that additional mandates be imposed on CI to ensure SCADA and/or telecommunications system security. This panel has heard my colleague's testimony about industry efforts already underway and the ideal role that the Federal Government should play. However, in an area as complex as homeland security, State and local governments and regulators look to the Federal Government for guidance on what constitutes reasonable investment. CI entities that invest in security measures meeting defined guidelines should expect to win cost recovery approval from State regulators. Federal guidance would facilitate investments not only by larger investor-owned utilities, but also by co-ops and municipals, all of which are faced with severe budget constraints and are under constant pressure to control rates.

Fifth, and finally——

Mr. PUTNAM. If you could just summarize.

Mr. KATZ. The plain fact, there is also a push on the part of many Federal agencies who believe that commercial wireless services can substitute for private internal networks. Quite frankly, they are even more vulnerable than anything that we could build ourselves. When power fails, it is commercial networks that go down first. Plus, they do not have a ubiquitous presence throughout an operating territory for any particular critical infrastructure entity, and they just cannot be relied upon. There is no exclusivity, no reliability, and no availability that is guaranteed to us.

This basically summarizes my comments, Mr. Chairman. I would be happy to answer any questions that you may have.

[The prepared statement of Mr. Katz follows:]

The U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on SCADA Security

March 30, 2004

Statement Submitted for the Record
By
Jeffrey Katz, Chair, Public Policy Division
United Telecom Council

INTRODUCTION

The United Telecom Council - UTC - is the telecommunications and information technology association that represents the interests of America's critical infrastructure entities. UTC and its association partners, the American Gas Association, the American Public Power Association, the Association of American Railroads, the Edison Electric Institute, the National Association of Water Companies, the American Petroleum Institute, the American Water Works Association, the Association of Oil Pipe Lines, the Interstate Natural Gas Association, and the National Rural Electric Cooperative Association, represent virtually every electric, gas and water utility and every communications network used to operate, control and maintain our nation's critical infrastructure (CI).

Some of us, at least, may remember a time when Americans could tolerate interruptions to the delivery of the critical infrastructure services delivered to them, such as electric power, natural gas, steam and water. Commerce and government continued to operate because paper and pencil recordkeeping was all anyone needed. Public safety agencies continued to operate because they used older telephone equipment that needed no external electric power. If their voice two-way radio system failed they could station patrol units at pole-mounted call boxes as a fallback. Things are very different today.

Today the very fabric of our nation depends upon the reliability and availability of services provided by America's critical infrastructure ('CI') industries. Every federal building, every military base, every railroad, every mass transit system, every telephone central office, every cell site, every traffic signal, every toll booth, every school, college and university, every hospital, every bank, every stock and commodity exchange depends upon an available and reliable supply of electric energy. Many also depend upon natural gas and water. If electric power fails, water service also can fail because water utilities use electric pumps to distribute water to consumers. Fire suppression efforts are impacted if hydrant service cannot be maintained. If electric power fails, central heating unit furnace blowers or boiler circulators cannot operate.

The services provided by CI no longer are mere conveniences whose loss we can tolerate. They are necessary for the health, safety and welfare of our nation and our people. Congress recognized this in the Balanced Budget Act of 1997 (P.L. 105-33) by determining that CI is a 'public safety radio service' under the provisions of the Communications Act of 1934 (47 U.S.C. 309 (j)(2) and FCC 00-403). Congress again acknowledged the importance of CI as a critical component of our nation's well being in Section 1016 of the USAPATRIOT Act.

Every CI entity depends upon telecommunications systems for SCADA, telemetry, command & control, remote actuation, and protective relaying operations. In addition, for both routine communications and during disasters and outages, CI entities depend upon private internal data and voice networks to direct the workforce and to restore service. To the extent that private internal communications systems are not available, reliable and exclusive, outages are extended; restoration is delayed; worker and public safety are compromised. In its January 2002 report on the current and future use of spectrum by the energy, water, and railroad industries, the National Telecommunications and Information Administration (NTIA) within the US Department of Commerce, recognized the importance of these systems in stating that, "the significance of these industries and the urgency of these issues [concerning spectrum use] may have changed as a result of the September 11th events. . . . . [I]t is of the utmost importance that the Federal Communications Commission revisit these critical [spectrum use] issues in order to accommodate the increasing role these industries play in maintaining quality of life."

POLICY ISSUES THAT NEED TO BE ADDRESSED

The overriding Issue that CI and Congress must address is: What federal or state policies, laws or regulations impact negatively CI's ability to avoid service interruptions, to reduce the duration and scope of service interruptions and to make CI, including its SCADA systems, less vulnerable to attack by non-physical intrusion? In many cases, these policies, laws or regulations actually run counter to homeland security objectives.

- **Public access to sensitive radio frequency information provides data useful to those who would do us harm. The federal system of record, the FCC's Universal Licensing System, is accessible by the general public via the internet. (47 CFR Sec 1.911).**

The FCC's Universal Licensing System (www.fcc.gov/wtb/uls) allows access to technical and location data regarding any FCC licensee. Anyone who would do us harm will find all they need courtesy of the FCC. It is time for the federal government not to be a willing partner in advertising vulnerabilities.

CI wireless SCADA, telemetry, command & control, data and voice systems can be compromised with the information contained within the FCC's public databases. A method must be found to make this information less public, either through creation of a confidential licensing category, or by providing the FCC with other authority, such as that enjoyed by NTIA, to exercise discretion concerning mission-critical telecommunication systems data. To that end, UTC urges greater flexibility be offered NTIA and the FCC in managing Federal and non-Federal spectrum use data, including providing NTIA with more flexibility for appropriate spectrum sharing with non-federal entities and thereby allowing greater confidentiality of licensing data.

- **Infrastructure data is made unnecessarily public through the FCC's pole attachment regulations and other provisions of the Telecommunications Act.**

Pursuant to the Telecommunications Act of 1996, maps of utility infrastructure must be made available to potential attachers upon the most minimal of showings, and those interested in attaching fiber-optic cable or other equipment to utility infrastructure are permitted to employ third-party contractors rather than personnel trained to observe strict safety regulations. Utilities are under significant pressure from the FCC to relax safety standards observed across the industry (the National Electric Safety Code, or NESC) for the purposes of telecommunications attachments to electric infrastructure. Indeed, language in a recent FCC attachment complaint decision dismissed a utility's concerns about the continued safety of its own infrastructure based on the lack of any serious accidents or harm thus far. One must wonder what the FCC is waiting to see happen before its attitude toward critical infrastructure protection changes.

- **Significant investment in better and more secure communications systems is hampered because such investments often are not immediately recoverable in rates and because the spectrum in which SCADA systems operate is not exclusive.**

Regulated entities are not able to recover capital investments through rate relief without filing a 'rate case' with state regulators. Rate cases are time consuming, tedious, and must be filed in each state in which the utility serves consumers. Further complicating the situation is the fact that most of our nation's utilities have a multi-state presence that would require consistent cost recovery schemes between and among the states.

Utility SCADA, telemetry, command & control, data and voice systems are system-wide, not statewide. Prudent and necessary investments in enhanced security, reliability and functionality should be recoverable immediately in rates, without the need to file a rate case in each state, and the specifics of the investment should be privileged and classified.

At the same time, why should private wireless SCADA systems be upgraded if the asset becomes stranded, due either to changes in the FCC regulatory environment or the possibility of co-channel or adjacent-channel interference? In many instances, utilities have been forced to operate wireless-based SCADA systems on bands where they have secondary status and may actually be required to shut down operations under FCC rules. Or they must operate these critical systems on bands shared with non-CI entities with little respect for FCC rules, creating interference and affecting reliability. This lack of spectrum exclusive to CI also serves as a disincentive to investment.

- **State and local governments should receive guidance from the Federal government as to the reasonable measures they can expect from industry.**

CI should be encouraged to adopt by a date certain voluntary industry standards (best practices) for telecommunications security. If such standards are not so adopted, then and only then, should standards be mandated by statute or by regulation.

UTC does not advocate that additional mandates be imposed on CI industries to ensure SCADA and/or telecommunications system security. This panel has heard my colleagues' testimony about efforts already underway and ongoing, and the ideal role of the Federal government in providing the small amount of funding needed to continue the work of the national laboratories and test beds. However, in an area as complex and large-scale as Homeland Security, state and local governments and regulators look to the Federal government for some guidance on the reasonable measures they can expect from industry. CI entities that invest in security measures meeting previously defined guidelines, should expect to win cost recovery approval from state regulators. Moreover, federal guidance would facilitate investments not only by large investor-owned utilities, but also by small municipals and cooperatives, all of which are faced with severe budget constraints and are under constant pressure to control rates.

A mandate would be even more likely to ensure cost recovery approval; however, the inevitable unevenness of applying government mandates among smaller entities, such as municipal utilities, co-ops and water systems, along with larger, multi-state entities, makes this solution undesirable.

- **Some federal agencies, including the FCC, erroneously believe that the communication needs of CI can be met by the use of Commercial Wireless Service ('CWS') providers such as cellular and personal communications services ('PCS').**

CI must work during times when utility services are likely not to be available, and their communications systems must withstand outages and storm damage. This is why CI entities build, own and operate their own private internal communications systems for

SCADA, telemetry, date, voice, and command/control of utility plant. And CI builds these systems so that they remain in operation for weeks under the worst conditions.

CWS providers, including cellular and PCS, generally have limited duration battery backup and are not designed to be continuously available or 100% reliable or exclusive. CWS does not provide ubiquitous coverage throughout a CI entity's operating territory. CWS builds its infrastructure where the revenue and subscribers are. CWS services are among the first to fail during a widespread power outage and, if they do not fail, they quickly become saturated as affected persons place calls or receive calls. CWS internal network latencies, which change over time and by subscriber link, prevent critical orders from being acted upon at precisely the same time by several different people at different locations.

August 14, 2003 probably is the most recent CI event. First, it is important to note that most if not all SCADA systems, including protective relaying, operated as designed. These systems protected automatically generation, transmission, switching station and substation assets from the effects of cascading outages and overloads. Second, while these systems automatically shut down utility plant in service, they are not designed to restore service after a blackout of such magnitude. Service restoration from cold start requires a carefully choreographed process involving hundreds of personnel at dozens of locations all performing specific tasks at precisely the right time. Coordination of that process and those players requires a voice communications system that is available to each of them and that does not have asymmetric network latencies. Utilities involved relied exclusively on their private internal systems. CWS had failed or operating cell sites were saturated. Wired telephone service was not available at each location. Cellular service, even if working, was not available at each location and the network latencies inherent in cellular systems was not conducive to the simultaneous execution of instructions.

Moreover, reliance on the "Wireless Priority Access System" (WPAS) is misplaced. WPAS does not afford CI the same availability, reliability and exclusivity as private wireless systems. First, WPAS must be applied for via rule waiver by a CWS provider under 47 C.F.R. Sec. 64.402 App. B. Second, WPAS has a hierarchy of access rights, with CI being 4th out of 5. Third, WPAS does not mean 'ruthless preemption'. Calls in progress are not interrupted. All WPAS does is bump a higher priority caller ahead of a lower priority caller in waiting for access. Fourth, CWS is among the first to fail in situations when CI needs communications most. and, since WPAS is CWS based, WPAS has no value. Fifth, WPAS anticipates normal cellular usage, it is not designed to handle 'dispatch' operations where instructions are issued that must be heard simultaneously by many people. WPAS offers nothing in the way of availability, reliability, and exclusivity.

In conclusion, UTC appreciates the opportunity to provide this statement to the Subcommittee. We would be pleased to provide any additional material that the Subcommittee may require for its deliberations.

Mr. PUTNAM. Thank you very much, and I appreciate your patience with the bells. And I appreciate all of your patience with the fact that we have three votes pending which will take about 30 minutes to handle. So with that, the subcommittee will recess. Feel free to get something cold to drink or hang loose and we will be back in approximately 30 minutes.

The subcommittee is in recess.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene.

I want to thank the witnesses for their patience and tolerance of the congressional voting schedule. We will go right into questions since we did complete the opening testimony before we recessed.

Let me begin with Mr. Weiss. When communication systems are installed in SCADA systems, how much consideration is given to security, in your opinion?

Mr. WEISS. Let me respond to the question with a question. What do you mean by "communication systems?"

Mr. PUTNAM. The method of transmission of instructions, the network connections.

Mr. WEISS. OK. In general, and I am going to give you a general statement that may not apply to everybody, and I am also phrasing it as a control system, not just a specific SCADA, usually security is not a critical aspect in a design of a control system. The implementation is usually most concerned with meeting performance specs. And the other thing that it is usually very much concerned with is the ability to communicate with the different systems that are being identified in that specification. There are very few specifications that include security.

Mr. PUTNAM. So very few considerations then are given to eavesdropping, disruption, issues like that?

Mr. WEISS. Correct.

Mr. PUTNAM. Mr. Freese, Mr. Katz, or Mr. Verton, would you like to add anything to that question? Mr. Freese.

Mr. FREESE. Yes, Mr. Chairman, I would. Although it is true historically that when it came to developing SCADA digital control systems, there was not security planned up front. But I know, speaking for AEP and a lot of other companies, we have since integrated security into all of those applications, as many SCADA systems as we possibly can because we do understand the need to secure those resources. So it has become now commonplace for a lot of companies to introduce security up front in the planning process, and then retrofitting on those areas that we did not have security prior to this.

Mr. PUTNAM. Mr. Katz.

Mr. KATZ. Thank you, Mr. Chairman. I think what we need to do is delineate a difference between then and now. A lot of legacy systems that are installed and still in place probably do not have a lot of security on them. To upgrade them would either mean replacing them or redesigning them and investing considerable dollars to do so. Newer systems that are being implemented take into account security concerns. They are generally taken into account in the RFP stage and all the way through.

But I am more concerned about the legacy systems and the fact that if we are going to upgrade, we do need to make a significant investment in that. And in the utility business every investment competes with every other one. Hierarchy is a priority. A substation transformer in danger of failure may cost $2.5 million to replace and that may end up displacing another project, because if you cannot capture the investment cost through a rate increase, then you need to do it either with cash-flow or bonds or stock and none of them is a particularly great alternative. But if it increases the reliability of the utility plant, it is something that we would rather see the ratepayers—I think any utility would rather see the ratepayers pay. But that takes a rate case and many BPUs and public utility commissions are reluctant to entertain rate cases except once every 5 or 6, or 7 or 8 years.

Mr. PUTNAM. What is the average age of a control system? Whomever may answer that one.

Mr. WEISS. The average age of a control system in a power plant is probably on the order of maybe 5 years old. SCADA systems in utilities, not in, if you will, the independent system operators because the ISOs are fairly new, but SCADAs in electric utilities are probably, again, just a rough order, probably 7 to 10 years old.

Mr. PUTNAM. And what about non-electric utilities—water control systems, flood control structures, things of that nature?

Mr. WEISS. At least in those that I have dealt with, a lot of these industries, particularly water, flood control, etc., in a sense just recently put in automation and so they have, if you will, newer systems. But here is the other thing I think that maybe is important to point out. In a control system, there are really two aspects. One is where the operator sits, that is usually a MicroSoft-based or a Unix-based operator screen. And in a spec, it is pretty straightforward, if you will, to specify that type of security. The other part of the control system is where you have the field devices, those things that actually measure temperatures, voltages, currents, and do the real-time calculations. That is where we really do not have the security technology at all yet. So putting that in a spec does not help. It does where you have the operator interface but not at the actual control. That is part of what I am hoping, and I am not speaking for anybody but myself, this is what I am hoping will come out of the National SCADA Test Bed.

Mr. PUTNAM. That was a point that I made in panel I, that the main facility is of less concern to me than the field facilities at the weir, at the dam, at the valve or the pump or whatever.

Let me followup on your point. A lot of those non-electric utility systems are only recently automated, meaning that they are newer, perhaps have more security hopefully built into them. But as a consequence, if there is a failure of those systems, have they removed the ability to manually override whatever it is, and are people adequately trained to do it the old fashioned way? Or are they out there with their palm pilots or their wireless or their computer and they are being told exactly which valve, which line, which wire, and, absent electronic assistance, they are unable to make whatever corrective actions they need to make?

Mr. FREESE. Mr. Chairman, if I may. In our remote substations, for example, we have a lot of them that require either an in person interface or some other type of control that can be used at a short range or short distance to be effective. Our people are trained in both the electronic means and the manual means. The problem with security, as you were mentioning at the remote substations, for example, or any of the substations that are equipped with data concentrators or RTUs are using computers. The problem with the more remote you get, the more difficult it is to keep security up to date; for example, antivirus, operating system patches, those types of things. So there is always kind of a lag between what needs to be done and what is done. And that is one of the focuses of the energy industry right now is to try to remedy that.

Mr. PUTNAM. Mr. Verton, you were very blunt in your assessment of where we are. Walk us through a plausible scenario for a terrorist act against using one of these control systems or SCADA systems, if you would.

Mr. VERTON. Well, Mr. Chairman, we have already seen some examples in recent history where disgruntled insiders have done things like let loose raw sewage by hacking into sewage treatment facilities in Australia. But my biggest point, I think the best example would be the August 14th blackout which, while it was not a deliberate act of terrorism, it was most likely a self-inflicted wound, if you will. The demonstration effect of what happened afterwards and the fact that these systems are vulnerable to electronic disruption means that we cannot discount a scenario that includes a deliberate disruption of electric power throughout a major metropolitan area of the country that is quickly followed up by a preplanned series of physical traditional terrorist attacks. For example, we saw thousands of people caught in the subway systems in Manhattan who were sitting ducks for a chemical or biological attacks. We saw people coalescing by the thousands on the streets who could have been the targets of a suicide bomber or something of that nature. So these types of scenarios are by no means what you might consider a Hollywood movie script. They are very much possible.

Also I might add, we started in the first panel talking about the physical vulnerabilities of these systems. The physical aspects of cyber terrorism are something that we have not paid a lot of attention to. But you can conduct the same sorts of denial of service attacks in an electronic sense by physically destroying key nodes in the electronic infrastructure. When certain nodes are taken off line, it could ripple out of control throughout other various portions of the infrastructure and other sectors of the economy. So you do not necessarily have to conduct an electronic attack sitting there with a computer, but you can, if you have access, physically destroy certain nodes and cause similar effects that you can then go ahead and take advantage of. Does that answer your question, Mr. Chairman?

Mr. PUTNAM. Yes. The counter argument to adequate preparation has been that the economic case just is not there for a number of local governments, municipalities, States, and private sector to invest in the security upgrades. Is that a flawed economic model, or is it an accurate economic model? And what could we do to encourage those investments in those upgrades? And I will begin with Mr. Katz and then work my way back toward Mr. Weiss.

Mr. KATZ. Speaking on behalf of the UTC and the industry in general, I think one of the things that the industry would not encourage are specific mandates to the industry about how to proceed with regard to investments in infrastructure. Certainly, if the industry were asked to come up with specific plans and guidelines or industry standards and best practices, that ought to happen within some reasonable timeframe.

But the real dichotomy here is that investment needs to be recaptured, money has to be spent, and it is real dollars. So you have to spend money and you better have the money to spend. So where do you get the money? If it is not through rate relief, or the sale of bonds, or the sale of stock, no one is going to just come over and hand us a bundle of money, and we are not asking for specific grants from the Federal Government either because we are the private sector. But if it takes that, we are certainly not going to turn it down.

The thing is that nobody really wants to be subject to mandated standards because the industry itself, the entire critical infrastructure component of the Nation is so diverse. A set of standards for a water company, a set of standards for electric companies, chemical, railroad, pipelines, you cannot adopt the same exact standard across the entire industry range. It is going to take some kind of voluntary cooperative effort on the part of Government and private sector in order to come up with a set of standards. That is the first thing.

The other thing is that if there is an uncertain regulatory environment with regard to the technologies that we implement, we do not want our assets or our investments to be stranded. So, for example, if there is really some good technology out there for wireless SCADA control, because we have point-to-point, end-to-end control over the infrastructure itself, as communications medium is independent of the common carrier, it is owned entirely by the critical infrastructure entity that is going to use it, so it is private wireless facilities, then the problem arises as to why was it exclusive, is it going to be subject to interference. Could some future regulation end up forcing us to compromise the security of that system simply because it is not really ours to use, it is part of some grant from a Federal agency, either the NTIA or the FCC. So it is a combination of factors and I am not really sure what the real answer is. But I think the industry itself needs to be given a chance to come up with a set of standards and best practices first, and perhaps a major investment in the INL labs is going to be very helpful that regard.

Mr. PUTNAM. Mr. Freese.

Mr. FREESE. I will go back to the budget question, the economic question. There are many companies, ours is one of them, who have expended millions in the last couple of years to improve security. Of course, we are going after cost recovery options with the States on these things and, again, we are trying to get people to listen to us based on tax incentives, things like that. However, I kind of go back to this is an awareness issue, first off. A company has to first of all have executive support for security, understand its responsibilities in the critical infrastructure organization. It is also an investor-incentive. At some point we are going to be judged on how secure is our company and how safe an investment is it in the face of all of the potential threats that are out there. To that end, we are following the NERC cyber security standards, first iteration of those, industry-based standards, and hoping to get other companies on board with those standards as well so we can all work toward information sharing, collaboration on security. I think budget is an important issue but a company that is serious about infrastructure protection will allocate funds for security, for both a business case and a security case.

Mr. PUTNAM. Does the cyber security take a backseat to physical security?

Mr. FREESE. It does not take a back seat. In our organization, we moved security out of IT and out of facilities, to both under risk management. So we are part of enterprise risk management right now. The budget is pretty much allocated among the two sectors and we have been doing a very comprehensive program of physical security upgrades for our substations and plants as well as cyber security upgrades of our SCADA systems. So we try to split it fairly equitably among both of those sectors.

Mr. PUTNAM. Mr. Weiss.

Mr. WEISS. I see three areas. Again, I am trying to answer more as a technologist, if you will. The first one is the business case. One of the most difficult things I have seen is that it is difficult for an executive to justify protecting a system if he does not think it is at risk. And that is such a great importance to the CERT for control systems. If an executive realizes that his system is at risk and systems like his have been compromised, there is much more of a reason that he would be willing to spend the money.

The second thing is that as technology stands today, there is not technology, as I mentioned, to secure the control system itself. What there is are, as mentioned, best practices. They are policies, they are procedures, they are audit functions, if you will, the low hanging fruit. The longer term is the work with the test bed to develop the technology.

The other piece, and I think this is important too because it is a big issue in the cyber world, we have a culture issue in many companies—this is not electric power, this is across the board—and the culture issue is between the IT organization and the operational organization. We need to figure out how to resolve that because many operational organizations feel that IT is more of a menace to them than somebody from the outside. And we need to be able to address that because IT has that security expertise. So it is, if you will, a multifaceted problem.

Mr. PUTNAM. Mr. Verton, what policies can be enacted that would encourage businesses to make the investment in security?

Mr. VERTON. Mr. Chairman, just to answer that question directly, I think the insurance industry in other sectors of the economy is already making great strides to offer favorable insurance rates to companies that meet certain standards and guidelines. There are one or two companies now that are offering those types of incentives. That is a type of effort that would do the one thing that is not happening right now, which is the national strategy to protect cyberspace only works if all of the infrastructure sectors are moving simultaneously forward. You cannot have one sector of the economy moving ahead of the others. So that is a type of a very simple way to get companies to apply these simple standards and practices.

Now if I could answer the previous question. My opinion is that the current economic model is flawed. I believe that the sellers will continue to sell what the buyers are buying. And the problem is that too much of the burden has been shifted to the end-user and the consumer of the technology as opposed to the developers. Right now the buyers are buying a lot of junk and they are being told to bear the burden to secure it after the fact. I know you are doing a lot of work on that particular type of issue, working with both the vendor and the end-user community.

Standards and best practices are fine but they only work when they are applied equally across the board. You cannot have a standard or a best practice that is not mandatory for everybody involved in this particular infrastructure. Somebody is always going to be somebody else's weakest link. So if they opt out, you have not really improved security for the entire infrastructure. In that regard, suggestions that cost money go nowhere unless you have some sort of mandatory requirement to meet some sort of standard. I find it very ironic that the only thing from what I can see that has resulted in an across the board, cross industry, cross sector improvement in security has been the one thing that the software industry and the hardware industry pretty much have been dead set against, which is regulation. Sarbanes-Oxley, HIPPA, and some other regulations have been the only thing that have really driven an across the board substantive improvement in security. And I think it is very ironic that the one thing that the developers of software and other technologies are dead set against is the only thing that seems to have worked so far.

Mr. PUTNAM. So you do not see an industry-based, volunteer, collaborative effort as being successful?

Mr. VERTON. No, I do not think I would go that far. But my opinion is that the private sector, when faced with tough choices, when it comes to making a choice between spending a lot of money that they cannot afford to secure the systems because they are being told that they own and operate a national security infrastructure, they need somebody to help them with that. The Government cannot tell them that it is their responsibility without saying and here is how we are willing to help you. Because private sector is not in the business of being defenders of America. This is an unprecedented situation in American history, in my opinion, that so much of our national security and our economic stability is in the hands of private companies. So if you are going to ask the private sector to bear the burden, you also have to come to the table with some practical suggestions on how that burden is going to be shared.

Mr. FREESE. Mr. Chairman, may I add something to that?

Mr. PUTNAM. You may.

Mr. FREESE. From the energy industry's perspective, we are not asking the Government to do everything for us or to give us all the money for all the security implementation we need to have done. We are asking to help prepare us for the extraordinary security event, extraordinary threat and attack on the energy industry. The other things we will take care of ourselves. But we try to get some assistance on the major upgrades, major changes across the industry.

Mr. PUTNAM. I hear what you are saying. But as somebody who is in business, granted, you have to meet a higher standard when you are a public utility or a private utility.

Mr. FREESE. Right.

Mr. PUTNAM. But at the end of the day, we have to strike some balance between addressing vulnerabilities and doing a good, thorough risk assessment and then trying to be all things for all potential threats. And I do not know where that line is. You squeeze the balloon here and you tighten up there, you dig deeper moats and you build taller fences, and then you have the cyber threat and so you move to the cyber threat, and in the meantime your fences have gotten rusty and your moats have filled in with sand and so you have to go back and dig those out deeper and replace the fence, and then technology has changed and everybody has gotten ahead of themselves, and then terrorists give up on attacking a new plant when all they really have to do is go into a shopping mall and use low tech devices that are being used in the Middle East on a regular basis.

As we wade through all this stuff and you start adding up what it would take to secure the magic 1,700 that DHS has now identified, knowing how many tens of thousands are not on that list, you are going to go out of business making yourself secure. You are not investing in R&D, you are not investing in upgrades of the service that is your core mission because every ounce of profit is going back into something that is not generating economic growth. It is a dead-end issue economically. So I do not know where the line is. You have an obligation to do certain things. But I do not know that you have an obligation to imagine every conceivable bad threat, malicious attack that a gazillion people are out there trying to think of against the United States. It just makes your head hurt, doesn't it?

What is the role of the Department of Homeland Security in this effort? And are they the right group of folks to fill this mission on the cyber threat, particularly on control systems?

Mr. VERTON. I will take that, Mr. Chairman.

Mr. PUTNAM. Go right ahead.

Mr. VERTON. Since I started the frontal attack, if you will, on DHS. My opinion has been pretty much the same as that of Mr. Richard Clark, you might have heard of him recently, that the position of cyber security has been, not the individual but the position, demoted. I think that right now the position is several layers down below where it needs to be. Basically, it has been removed from a Presidential advisor role to an advisor to an Assistant Secretary level. And I do not think that Mr. Yoran at the moment has the ability to see things that need to be fixed and take immediate action. So I think there are still some thought that needs to be given to the current organizational structure of DHS, particularly with respect to the role of cyber.

Mr. PUTNAM. Is there a Presidential level advisor on chemical-biological-radiological-nuclear devices?

Mr. VERTON. I believe there is still a Presidential level advisor for terrorism. The problem being, if I know the history correct, as Mr. Clark has told it, a special position was created for cyber terrorism that was recommended by Mr. Clark and he I think had every intention of remaining a Presidential level advisor until the DHS proposal came around and it was placed in the DHS, unfortunately not up at the secretary level but several layers below.

Mr. PUTNAM. I think it is real easy to get hung up on what the flow chart is instead of what the mission is.

Any other thoughts on that, Mr. Weiss?

Mr. WEISS. Yes. My thoughts are a little bit different. Control systems are not unique to any single industry. To be able to protect control systems, that function needs to reside in whatever organization has the widest breadth to cover the most industries. DOE's function is really energy. But the same, for example, Honeywell control system that is in a power plant is also in a refinery, it is also in a water plant, it is in a chemical plant, it is in a paper mill. So I am really giving you more of a question back. But the real issue in where this needs to reside is what is the organization that will really cover the industrial infrastructure because that is where the vulnerability lies.

Mr. PUTNAM. Within the overall universe of cyber threats, are threats to SCADA systems the greatest of cyber threats because of their connection to the physical infrastructure?

Mr. WEISS. Again, I am going to answer this as a control system engineer. The reason I believe that cyber threats are, if you will, critical to control systems, our control systems were not designed to be protected from them. So what is happening is you have a much less resistant system. It is also a system that has a lot higher consequence if something happens to it. I hope, because I am not a policy person, that the number of threats to these systems are much less than they are to other places. But the other systems, in general, have been designed or supposedly have been designed to resist those other threats.

Mr. PUTNAM. Mr. Verton.

Mr. VERTON. Mr. Chairman, I will answer that question from a terrorism perspective. I think the answer is absolutely yes, only because any time you have computers that control real things in the real world that have public safety implications, they inherently immediately become a potential target for terrorists. So I think my technical colleagues on the panel would agree that description fits the bill for SCADA systems, if you will, across industries. So, yes, I think from a terrorism perspective, they are a primary national security concern.

Mr. PUTNAM. Mr. Freese.

Mr. FREESE. I agree with Mr. Verton. Again, a lot of the energy industry agrees with Mr. Verton because they are trying to secure their control systems as much as they can. It is a huge task and it is going to take a long time.

Mr. KATZ. I would agree with that, too. From the perspective of critical infrastructure industries, the threat to SCADA systems and command and control systems is probably much greater and would have greater consequences than threats to our standard traditional data processing systems.

Mr. PUTNAM. How helpful would a SCADA-specific cert be?

Mr. WEISS. I believe from all of the meetings I have had with different industries, through ISA, through IEEE, through all of these different organizations, when the concept of a cert from control systems is brought up, it is almost always on the top of the list of what they think would be most helpful.

Mr. PUTNAM. Does everyone agree with that? OK. Let the record reflect that everyone agrees with that.

Let us talk about public disclosure. I am going to start with the reporter on this one. I always love hearing their views on open records. Telecom systems use control systems that require the public spectrum, that is an FCC issue, disclosure is an important part of it. As you know, blueprints, plans, designs, electrical wiring, circuitry, everything is generally available and easily accessible. What are your thoughts on restricting that?

Mr. VERTON. Mr. Chairman, I am obviously interested as a journalist, somebody who would be interested in finding this information and publishing it. But there have been many cases where I have not published information because of my own concerns and understanding of the damage it could do. Now I may be unique among journalists in that respect.

I think there is a lot that can be done about restricting not necessarily the disclosure of the information, but how it is communicated to the people that need to know it. Let me give you some examples of some very recent post-September 11 security assessments that were done just on public Web sites for major, major corporations in, of all places, Lower Manhattan. A CIA psychological profiler was hired to do a study of the Web sites of various large Fortune 500 companies to find out to what extent the content of their Web sites would make them targets of Al Qaeda. This particular survey found detailed maps and drawings of air conditioning and ventilation systems for large office complexes, it found the load bearing capacities of elevators, it found private data on some of the senior executives, the number of people present at any one office facility and where they worked, some banks had posted, for example, notices that they had frozen Al Qaeda related bank accounts for the world to see, support for globalization issues which we know has been known to stimulate portions of the Al Qaeda network.

So there needs to be a business case and a balance struck between what you post on the Internet and maybe how you communicate it to the people who need to know certain information. For example, a local community has every right to know that they are living within striking distance of a dangerous chemical facility. They want to know that their children are potentially in danger. But do we need to post, for example, detailed information on that facility to the people in that particular community. Do we need, for example, to post detailed information on a uranium mining facility so that a potential terrorist could figure out how to do the most harm. And that is the balance that needs to be struck.

From a private sector perspective, the companies that own and operate the critical infrastructures need to take a look at what they are putting out in the public to determine whether or not it serves their business. If it does not serve their business, they need to start asking themselves hard questions as to why are we putting it out there to begin with. And a lot of these companies fall into that first category of putting our air conditioning and ventilation diagrams for their office complexes. It makes absolutely no sense from a sales or a marketing perspective.

Mr. PUTNAM. Does the public have a right to know that there is a site in their community that is 1 of the 1,700 identified lead targets?

Mr. VERTON. I think a community has a right to know if that 1 of 1,700 is a dangerous chemical facility or a nuclear reactor of some sort. Certainly, they have a right to know that they are living within a danger zone. The question becomes how do you communicate that to the public and to what level do you communicate that information. I found, for example, I found a map of the entire United States with the locations of all spent nuclear fuel storage facilities on the Internet. Did that need to be up there post-September 11? I am not sure. To my knowledge, it was eventually taken down by the Department of Energy. So that is the type of balance we need to strike, in my opinion.

Mr. PUTNAM. Our right to know in the past, particularly with the types of sites we are talking about here, was driven by environmental concerns. And now we are talking about terror threat-based concerns which are somewhat different. You have a right to know if a particular chemical plant is discharging X number of pounds of sulfur per year that has been known to have a connection to higher incidents of cancer or whatever. All that kind of stuff that is imbedded in our environmental law. But what are the consequences of letting the world know what we think the top 1,700 are; meaning that everything that is not on the top 1,700 has a lesser degree of preparation or prevention, and what effect does that have on your business. Obviously, if you run a nuclear plant, I do not think being on the top 1,700 is going to be a surprise to anyone. It is not going to affect your insurance rate and it is not going to affect who your neighbors are; they are pretty well aware of what they bought into when they moved to the neighborhood. But the rubric that they used was public health and safety, economic, which is very nebulous, symbolic, which is extraordinarily subjective and nebulous, and national security, which that ought to be fairly identifiable. But people living next to a tourist attraction might think that is a pretty good thing, not realizing that it also might be a target for terrorists.

So, as we move down this road, and I wish there were Members here from the other side of the aisle because they have an outstanding record, as do most Members of Congress, pushing for increased public disclosure, a very rigid FOIA law. But as we deal with these new issues, we have to have this debate. And I do not know where we end up.

Mr. Katz.

Mr. KATZ. Thank you, sir. It is part of the dichotomy of the entire process; and that is, yes, the public is entitled to know certain things that may harm them, and at the same time there is certain information that we make available because it is required to be made available that can fall into the wrong hands and be used against us. For example, Mr. Verton refers to why would a utility market anything that deals with its infrastructure and its office building about air conditioning systems. Well, it does not do that. If we are building an office building, at least in my State, we are probably going to have to get local land-use approval, we are going to be before a planning board or a zoning board of adjustment. Once that is approved, now we are going to have to file plans with the building department and secure all proper permits. So all of those mechanical drawings, all of the electrical infrastructure, everything about that building is now public record because it is in the building department in the municipality that is issuing the permits. So that is a public record. Anybody who wants to find that can go get it.

We have Federal agencies that we need to deal with that also discloses information to the public. At the same time, we all comply with SARA Title III. And in the local level, every business and industry in a community has to report to its local Office of Emergency Management once each year all of the chemicals and hazardous substances that it has onsite. That is available to the public and it is also available to anybody who wants to go break in to those facilities to be able to steal harmful materials and use them against us.

So, yes, I agree that there is a need for public disclosure. As a former chief executive officer of a municipality, yes, the public should know these things. But to what extent do we let them know about certain things that could be used against us in a manner that hurts a lot of people. And that is a wonderful policy issue for Congress to deal with, and, Mr. Chairman, I wish you an awful lot of luck with that. But, yes, it is there and I think we all recognize it.

Mr. PUTNAM. At what point does disclosure become harmful in and of itself.

Mr. KATZ. Exactly.

Mr. PUTNAM. Disclosure is intended to protect the public from harm. But at what point does disclosure become harmful. And that is clearly something we are going to have to deal with. I do not know what ill purpose the public is served by not having access to the blueprint of a nuclear power plant. I cannot think of how the public is poorly served by not knowing that, or knowing the precise latitude and longitude of switches and valves and everything else. But I am sure that there are plenty of people who would be happy to tell me what they are.

At this point, we are going to bring this in for a landing. I want to give all of you the opportunity to give closing remarks, deal with any issue that you came prepared to discuss that we did not get to, or add your closing thoughts on the topic in general. We will begin with Mr. Weiss and move down the table.

Mr. Weiss, you are recognized.

Mr. WEISS. First of all, I wanted to thank you for inviting me here. I very much appreciate that. I also appreciate that this discussion itself took place. I just want to reiterate three things. One is that control systems are truly important but security was never a basic premise when they were designed. They need to be protected. The second part is that there really needs to be a business case for their protection. And that is part of where that e-cert comes in. The third part is we need an adequately funded test bed for, if you will, the entire infrastructure to be able to evaluate and develop and demonstrate technologies to secure these, and, to me, that is the SCADA test bed. So, thank you.

Mr. PUTNAM. Thank you. Mr. Verton.

Mr. VERTON. Mr. Chairman, thank you very much again for having me here today. I will just close by saying that I feel that these are very dangerous times for us post-September 11 because I think we are entering a phase where we are potentially becoming dangerously complacent because of the fact that nothing has happened since September 11. Particularly in electronic realm of this problem, the threat of cyber terrorism, as we have been discussing today, faces a very significant perception problem because people do not think that people who are trying to kill us are interested in these tactics, they do not think that they are capable of it. I have documented plenty of instances arguing the opposite point of view in that. I will just say that I think this is an urgent national security matter. Also, I would hope that the private sector gets some sort of real practical assistance in this effort to make sure that these systems are secured in a way that works for everybody.

Mr. PUTNAM. Thank you. Mr. Freese.

Mr. FREESE. Taking the information disclosure one step further, a lot of the discussions earlier from the Government side focused on industry and Government cooperation, providing information to each other to help secure the critical infrastructure. But I think it needs to go further. Right now, I think there needs to be a better awareness between Government and industry of what the scope of the threat really is. I think they have to make a joint commitment that they have to work together, not just lip service like we have always heard, but something that is concrete, some kind of a plan that we will work together. This will require better information protection for information submitted from utilities, between utilities, to the States. All of those things have to be addressed. Right now, a lot of the blockage on getting things done—for example, the 1,700 list from the States is derived in a lot of cases without energy companies or other infrastructure organizations providing what they consider to be critical. The State says I think that is critical, let's send it in. They ask the infrastructure organizations for information. How can you protect my information if I give it to you? If you cannot, I cannot provide it. So there is kind of a roadblock there. We need to eliminate that roadblock as soon as possible.

Mr. PUTNAM. Mr. Katz.

Mr. KATZ. I agree, gentlemen. So I am not going to duplicate that. On behalf of UTC, I would just like to thank the committee for its time and attention to this matter. I think it is extremely important to all of us. It is certainly important to the critical infrastructure industries. And one of the areas in which the Federal Government could really be helpful is if there could be just one Federal agency with accountability and responsibility to push this effort through. Right now, DHS is still organizing itself, the other independent Federal agencies do not see a lot of these issues as in their ballpark or part of their jurisdiction. So it would be very, very helpful if there was one point of contact within the Federal Government for all of this in cyber security.

And I agree with Mr. Verton. I think the level of attention that needs to be paid to cyber security at the Executive level probably needs to be raised. With the departure of a cyber security czar, it probably is not there anymore. And I realize there are a number of national priorities and this is just one of them. But it is an important one and you have the folks here who are involved with that on a day-to-day basis and we recognize it as being important. But we do need some Federal leadership on this and the public sector will help and the private sector will cooperate to the extent that it needs to in order to get the job done because it helps all of us.

Mr. PUTNAM. Thank you, all of you for your comments. I would urge you to keep DHS' feet to the fire and help us do the same. At some point the excuse that they are a new department will cease to be valid. It has already reached that point with me. It is no longer an issue. They have had their 1 year anniversary, they have cut the cake, and now no more excuses.

So we thank all of you very much for your candor and insight and for your patience with the disjointed nature of this hearing. I also want to thank Mr. Clay and Mrs. Miller for their participation and interest in this issue.

In the event that there may be additional questions that we did not have time for today, the record will remain open for 2 weeks for submitted questions and answers.

With that, the subcommittee stands adjourned.

[Whereupon, at 5:17 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

The U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on
Telecommunications and SCADA: Secure Links or Open Portals to the Security of Our Nation's Critical Infrastructure

March 30, 2004

Supplemental Statement Submitted for the Record
By
Jeffrey Katz, Chair, Public Policy Division
United Telecom Council

INTRODUCTION

The United Telecom Council - UTC – was honored to testify before the Subcommittee regarding the interdependencies between the supervisory control and data acquisition (SCADA) networks and telecommunications functions that underlie the operation and maintenance of our Nation's critical infrastructure (CI). Based on the testimony of witnesses during that hearing as well as the Members' questions to panel participants, UTC would like to provide the Subcommittee with additional information relevant to its avenue of inquiry.

FCC

In its written and oral testimony, UTC provided its recommendations concerning federal or state laws, policies or regulations that may serve to make SCADA systems more vulnerable to attack or compromise. Because these are telecommunications-based systems, many of the recommendations centered on regulations promulgated by the Federal Communications Commission (FCC) in effectuating policies enacted by Congress. These recommendations were not intended to be criticisms of the FCC, but examples of the lack of appropriate regard to the importance of private, internal radio systems to the security of CI operations. While valid policy directions may have led to existing rules and administrative systems, a better balance now should be struck, especially following the events of September 11th. The examples provided were meant to place in sharp contrast the agency's 1) mandate to maximize the use of radio spectrum as a public resource (in no small part driven by budget concerns) which drives its deference to commercial systems and its management policies encouraging access to frequency licensing information; with its 2) resulting insufficient consideration of the CI network security implications of these policies.

In particular, UTC submits these supplemental comments to further elucidate its concerns about current proceedings that may have a dramatic impact on CI network security. In addition, we believe that the Department of Homeland Security (DHS) should provide a countervailing force to the currently unchallenged jurisdiction of the FCC over aspects of CI operations: the management of spectrum used by the CI for its critical functions, the safe use of CI infrastructure elements by telecommunications service providers, coordination of other federal and state agency CI communications requirements and the safety of CI emergency response personnel and the public in general.

Interference Temperature Proceeding

We understand that spectrum management and allocation policies are not within the purview of this Subcommittee; however, we believe that certain proceedings should be brought to the Subcommittee's and thereby the full Committee's attention that are indicative of current dangers to CI telecommunications networks. A good example of this is the FCC's "Interference Temperature" Notice of Inquiry/Notice of Proposed Rulemaking (ET Docket No. 03-237), which proposes to implement a yet-undeveloped technology to permit new, unlicensed users within close range of CI microwave systems in the 6 GHz and 12/13 GHz bands, causing harmful and destructive interference. Without these dependable communications links, the power industry would be unable to operate, as they control the nation's energy systems in a safe, timely and economical manner.

Interference is presently minimized through coordination of the frequency, radiated power and location of individual transmitters. Several methods are proposed for determining and monitoring interference temperature, but there is no guarantee that any of these theoretical systems will work or that licensed systems will not receive harmful interference. Because new users would be unlicensed, locating each offender and resolving interference would be an impossible task.

Interference to these critical microwave network systems could place the entire energy system in jeopardy. Moreover, this regulatory uncertainty acts as a disincentive to invest in newer, improved equipment because they may become stranded investments due to a change in FCC policies. The FCC must recognize that the importance of CI systems should weigh heavily in this and any other proceeding; interference cannot be tolerated given the potential impact on all sectors of the Nation's security and economy.

800 MHz Proceeding

Another example of a threat to CI communications systems is evident in the controversial 800 MHz proceeding. To solve the growing interference problem between low-site, cellularized digital and other systems in the 800 MHz band, a complex rebanding proposal is currently under consideration. It is estimated that this proposal would take at least four years to complete (not including probable court challenges), during which time interference to CI communications systems would continue to increase. The length of this proceeding – already more than two years old – also has caused uncertainty among CI entities planning major investments in telecommunications infrastructure.

While it is beyond the scope of these comments to discuss the details of the proceeding, it should be noted what the FCC's decision must do to protect mission-critical CI systems. CI systems must be able to continue to grow to meet new infrastructure pressures as populations and communities grow; they cannot be "frozen" for any length of time or denied access to additional spectrum. Any rebanding process must include reimbursement for all costs and the reliable operation of radio systems at all times. Finally, in keeping with FCC spectrum policy, the Commission should continue to encourage all users of this important frequency band to migrate to better spectrum efficiency and more advanced technology, without restricting such growth to commercial carriers.

ROLE OF THE DEPARTMENT OF HOMELAND SECURITY

The written testimony and response to questions from the Subcommittee provided some encouraging information about the need to focus on cyber security as it relates to SCADA and the security of the CI communications systems in general. We believe that there are three issues that warrant greater attention.

First and foremost, cyber security does not seem to enjoy the appropriate level of priority within the Department's organizational structure: it is only a division under an Assistant Secretary. Given the fact that the security of our cyber systems is at the core of all other critical infrastructure protection measures, consideration should be given to focusing greater Department resources in this area.

Second, the organizational structure of the Department itself seems to create artificial divisions between critical infrastructure protection, cyber security and SCADA security. Divisions and departments dealing with these issues are located under several different directorates, as well as in special assistant offices that report directly to Secretary Ridge. This structure would seem to discourage cross-sector coordination within the Department itself and amongst the sector ISACs, and promotes an unnecessarily inefficient and "stovepipe" information flow. Indeed, UTC has been unable to find an ISAC willing to include CI telecommunications issues within its scope of concerns.

Finally, SCADA and other private communications networks are used by all segments of the CI for system monitoring and grid protection, including the water industry for both supply and quality purposes, the oil and gas industry for production, supply and delivery purposes, by electric utilities for transmission and generation protection, and by nuclear power plants. Each of these industry groups is subject to diverse state and federal agency regulations pertaining to safety and service reliability, most of which require reliable communications networks for compliance.

These regulations include:

- The Pipeline Safety Act administered by the Department of Transportation's Office of Pipeline Safety, which requires gas pipelines to establish emergency plans that include adequate means of communications with fire, police and other public offices for the emergency shutdown and pressure reduction in any section of a pipeline.
- Water quality standards administered by the Environmental Protection Agency.
- The Federal Emergency Management Agency's (FEMA) "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Plants," which require utilities to have "reliable primary and backup means of communications" and to prepare an emergency plan to include use of these communications between a nuclear facility and the utility's near-site emergency operations facilities, state and local emergency operations centers and radiological monitoring teams.
- FEMA specifications in its "Functional Criteria for Emergency Response Facilities," stating that reliable primary and backup means of communication are necessary among the Emergency Operations Facility, Technical Support Center, Nuclear Regulatory Commission and state and local emergency operations centers. The reliability of the chosen communications systems must be demonstrated under emergency conditions, which generally rules out commercial wireless services due to their lack of reliability during power outages.
- The North American Electricity Reliability Council (NERC) standards, which require "reliable and security telecommunications networks" and the use of exclusive telecommunications channels between the system and control centers of adjacent electric systems.
- State public service commissions' requirements that utilities respond to reports of downed electric lines and gas leakages within 30 minutes; this requires interference-free communications capabilities with emergency field crews.

DHS could provide a very valuable function by coordinating all the CI communications network requirements, not just SCADA, of Federal and State governments, and working with industry to eliminate corresponding vulnerabilities. All of CI would benefit from the development of a comprehensive cross-sector frequency management and licensing scheme that recognizes the security needs of each of these sectors. These issues should be addressed in the comprehensive national infrastructure plan that DHS intends to complete by December 2004

As the only trade association devoted to the telecommunications and information technology interests of critical infrastructure entities, we welcome the opportunity to work with DHS as a conduit of vulnerability assessment information and recommended security measures to our members. We look forward to working with the Subcommittee to establish the appropriate contacts within DHS to provide this important function.