AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SCADA SYSTEMS AND THE TERRORIST THREAT: PROTECTING THE NATION'S CRITICAL CONTROL SYSTEMS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE 0PROTECTION, AND CYBERSECURITY

WITH THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, SCIENCE, AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

OCTOBER 18, 2005

Serial No. 109–45

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

32–242 PDF WASHINGTON : 2007

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 HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
PETER T. KING, New York *(Ex Officio)*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

SUBCOMMITTE ON EMERGENCY PREPAREDNESS, SCIENCE, AND TECHNOLOGY

DAVE G. REICHERT, Washington, *Chairman*

LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, New York *(Ex Officio)*

BILL PASCRELL, JR., New Jersey
LORETTA SANCHEZ, California
NORMAN D. DICKS, Washington
JANE HARMAN, California
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity:
Oral Statement 1
Prepared Statement 1
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity 2
The Honorable Dave G. Reichert, a Representative in Congress From the State of Washington, and Chairman, Subcommittee on Emergency Preparedness, Science, and Technology:
Oral Statement 2
Prepared Statement 3
The Honorable Bill Pascrell, Jr., a Representative in Congress From the State of New Jersey, and Ranking Member, Subcommittee on Emergency Preparedness, Science and Technology:
Prepared Statement 3
The Honoralee Peter T. King, a Representative in Congress From the State of New York, and Chairman, Committee on Homeland Security:
Prepared Statement 4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Oral Statement 5
Prepared Statement 58
The Honorable Donna M. Christensen, a Delegate in Congress From the U.S. Virgin Islands 67
The Honorable Norman D. Dicks, a Representative in Congress From the State Washington 68
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina 65
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 64
The Honorable Eleanor Holmes Norton, a Delegate in Congress From the District of Columbia 62
The Honorable Stevan Pearce, a Representative in Congress From the State of New Mexico 56
The Honorable Ginny Brown-Waite, a Representative in Congress From the State of Florida 60

WITNESSES

Dr. K.P. Ananth, Associate Laboratory Director—National and Homeland Security, Idaho National Laboratory:
Oral Statement 24
Prepared Statement 25
Mr. Alan Paller, Director of Research, The SANS Institute:
Oral Statement 40
Prepared Statement 42

Page

Mr. Donald "Andy" Purdy, Acting Director, National Cyber Security Division, U.S. Department of Homeland Security:
Oral Statement 6
Prepared Statement 7
Dr. William Rush, Institute Physicist, Gas Technology Institute:
Oral Statement 31
Prepared Statement 33
Mr. Larry Todd, Director, Security, Safety and Law Enforcement Bureau of Reclamation, U.S. Department of the Interior:
Oral Statement 14
Prepared Statement 15
Dr. Sam Varnado, Director of Information Operations Center, Sandia National Laboratory:
Oral Statement 16
Prepared Statement 18

APPENDIX

Dr. K.P. Ananth Responses to the Honorable Daniel E. Lungren Questions 71
Mr. Donald "Andy" Purdy Responses to the Honorable Bennie G. Thompson Questions 81
Mr. Larry Todd Responses to the Honorable Bennie G. Thompson Questions .. 86
Dr. Sam Varnado Responses to the Honorable Bennie G. Thompson Questions 89

SCADA SYSTEMS AND THE TERRORIST THREAT: PROTECTING THE NATION'S CRITICAL CONTROL SYSTEMS

Tuesday, October 18, 2005

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
WITH THE
SUBCOMMITTEE ON EMERGENCY
PREPAREDNESS, SCIENCE, AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 4 p.m., in Room 311, Cannon House Office Building, Hon. Dan Lungren [chairman of the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity] presiding.

Present: Representatives Lungren, Reichert, Pearce, Brown-Waite, Pascrell, Thompson, Dicks, Norton, Jackson-Lee, Christensen, Etheridge and Sanchez.

Mr. LUNGREN. The joint hearing of the Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity and the Subcommittee on Emergency Preparedness, Science and Technology will come to order. The subcommittees are meeting today in joint session to hear testimony on supervisory control and data acquisition systems, better known as SCADA systems, in the effort to protect these critical control systems from terrorist attack.

We have been informed that we will have votes starting at approximately 4:30, and as a result, we are going to have a major interruption. We have six major witnesses here on a very important matter, so I am going to not give my opening statement. It will be included as a part of the record. And then we will proceed.

PREPARED OPENING STATEMENT OF THE HONORABLE DANIEL LUNGREN

Good morning and I would like to welcome everyone to this joint hearing of the Committee on Homeland Security's Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity and the Subcommittee on Emergency Preparedness, Science & Technology. I thank Chairman Reichert and Ranking Member Pascrell for agreeing to hold this jointly, as this critical issue has far reaching impacts.

We convene today to focus on the protection of control systems at our Nation's critical infrastructure. Control systems are utilized in a wide variety of industries—such as electrical generation and distribution, oil and gas systems, traffic signals and other transportation supervision, water management (including dams), and manufacturing industries. These control systems are commonly referred to as SCADA systems.

These computer terminals have the ability to give supervisory control to a central user over separate and often disparate functions or processes. Further, SCADA systems collect information from remote locations and coalesce it into one location.

Now what does this actually mean? Simply put, a manufacturing facility or any of the forementioned facilities incorporate many different processes and functions. To safely, securely, and efficiently run the facility, companies must be able to monitor and adjust these processes simultaneously. Before SCADA systems, workers would be placed throughout a facility and manually monitor and adjust the various systems. SCADA systems bring monitoring and control of these functions into one centralized location, making it easier and more efficient to run these processes.

At the same time, these systems present serious security challenges. Because these terminals control crucial systems within our critical infrastructure and are often connected to networks and can be remotely accessed, they present an attractive means for those wishing to cause harm and confusion.

Securing SCADA systems is similar to securing all of our cyber infrastructure; however, the consequences are potentially very different. Minimally, adversaries could target SCADA systems through cyber networks, utilizing common cyber attack methods to render the SCADA systems unusable. This could slow down, stop, or endanger the functions of the facility. This would result in not only serious problems at that facility but potential cascading effects on other facilities or processes that are dependent on the attacked facility. Even worse, terrorists could utilize SCADA systems for their own sinister motives—causing a pipeline to burst, opening flood gates on dams, or shutting down our electric supply, all without ever gaining access to the facility.

Part of this hearing will be to understand the function of these systems within the greater picture of our critical infrastructure and to understand the general vulnerabilities, consequences, and interdependencies of these systems. Although there are literally thousands of SCADA systems across the U.S., not all of these control systems involve industries or facilities that would be considered high risk.

The threat to these systems has long been recognized and the Federal government, the private sector, and this country's best minds have been working for years to address it. The second part of this hearing then, is to understand what progress has been made—at all levels—to address these vulnerabilities.

We have a diverse panel of experts today, representing the Federal government, the National Labs, the dam industry, the gas industry, and the cyber industry. I look forward to hearing from all of you about your ongoing efforts, and your views on what we need to do to further assist you in addressing SCADA security.

I am especially interested in hearing about the status of securing our dams. We have seen recently in New Orleans what can happen when nature overwhelms us, even with days of advance notice. The potential consequences of an unanticipated attack could be far worse.

Again, I thank all of our witnesses for being here. I now recognize the Ranking Member of the Subcommittee, the Gentle Lady from California Ms. Sanchez, for any opening statement she'd like to make.

Mr. LUNGREN. The Chair would recognize the Ranking Minority Member of the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, the gentlelady from California Ms. Sanchez, for any statement she may make.

Ms. SANCHEZ. Thank you, Mr. Chairman. And considering I am under the weather today and we are pushed against votes, I, too, will hold my opening statement and submit it for the record so that we can hear from the witnesses today. Thank you.

Mr. LUNGREN. I thank the gentlelady, and her prepared statement will be made a part of the record.

The Chair would now recognize the Chairman of the Subcommittee on Emergency Preparedness, Science and Technology, the gentleman from Washington Mr. Reichert, for any statement he may make.

Mr. REICHERT. Thank you, Mr. Chairman. I, too, will withhold boring you to death with my opening statement, and we will ask

that it be placed in the record. Thank you, and welcome to the witnesses today.

[The information follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE DAVID REICHERT

Thank you, Chairman Lungren. I would also like to welcome everyone, especially our witnesses, to this joint hearing.

We are here today to discuss a topic that affects our everyday lives, although many of us are never aware of it. Process and control systems and the operations that they manage are critical to our Nation. They enable us to have everything from clean drinking water and fuel for our cars to electricity in our homes.

As a former law enforcement officer, I know firsthand that prevention is the best way to save lives and protect property. So, I am particularly interested in our Nation/s efforts to secure these systems.

But, I also recognize that we can not expect to prevent every attack, especially in an environment as open and free-flowing as cyberspace. And, as we have seen in the aftermath of Hurricane Katrina, our ability to recover from an incident—whether natural or manmade—can be just as important as our ability to detect and prevent it from happening in the first place.

Part of the mission of the Department of Homeland Security's National Cyber Security Division is to "establish a National Cyberspace Response System." Ideally, such a system will rapidly identify and respond to cyber incidents and help mitigate against any damage caused by malicious cyberspace activities.

So far, we have fortunately not yet experienced a serious cyber attack directed at the control systems that manage our Nation's electrical grid, dams, and other critical plants. Undoubtedly, at some point, our luck will run out. That is precisely why we must continue to emphasize prevention and response and develop more robust SCADA software technology.

I am, therefore, keenly interested in learning more about the vulnerabilities of our SCADA systems, what the NCSD—in partnership with the National labs and the private sector—has done to address such vulnerabilities, and the additional steps that need to be taken to establish and implement a cyber response system.

Again, I want to thank all our witnesses for being with us today. I look forward to your testimony on this important issue.

Thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. LUNGREN. All members of the committee—the Chairman would recognize the Ranking Minority Member of the Subcommittee on Emergency Preparedness, Science and Technology, the gentleman from New Jersey Mr. Pascrell, for any statement he might make. I would just inform the gentleman that we have all waived our statements, but the gentleman may proceed as he wishes.

Mr. PASCRELL. I will waive it.

Mr. LUNGREN. Your statement will be made—a prepared statement will be made a part of the record.

[The information follows:]

PREPARED STATEMENT OF THE HONORABLE BILL PASCRELL, JR.

I want to thank Chairman Lungren and Chairman Reichert for holding a hearing on an issue of vital importance to our national security.

Indeed, protecting America's critical control systems is a topic that, I believe, has not received the attention it deserves. We *know* that vulnerabilities within these systems are abundant, and we *know* that the threat of a terrorist attack against these systems is real.

Congress needs to engage in robust analysis and oversight in this realm; we need to help *ensure* the security of the various control systems that are used in critical infrastructure—and I am heartened that today two Homeland Security subcommittees are leading the charge.

Obviously this is something that affects all of us. But as a resident of New Jersey, I must say that this issue particularly resonates with me.

There are a number of areas in my state, for example, that contain key assets on which the region's economy and community functioning depend—including crit-

ical utilities that provide gas, electric power, water and telecommunications services.

A cyber attack on one of New Jersey's four nuclear power plants, or *100 chemical sites,* for example, has the potential to be absolutely devastating. Not only in terms of lives lost, but also in the regional and national economic destruction it could bring forth. This is serious, serious business.

Back in 2002, the National Infrastructure Protection Center reported that a computer belonging to an individual who had links to Osama bin Laden contained programs that *clearly* showed the individual's interest in the structural engineering of various critical infrastructures.

It also indicated that al-Qa'ida members had sought information about control systems from multiple websites.

With this knowledge, one would assume that Washington would take every appropriate step, take every possible measure, and institute every conceivable action to ensure that critical infrastructure would be greater protected.

Inexplicably, this doesn't seem to be the case.

In fact, DHS as a whole has been slow in completing its critical infrastructure protection policies.

In December 2003, President Bush issued Presidential Directive 7, establishing a national policy for federal departments and agencies to prioritize critical infrastructure. DHS was charged with developing the National Infrastructure Protection Plan (N.I.P.P.) to serve as the guide for protecting infrastructure.

The N.I.P.P. was *due* in December 2004. In February 2005, an "Interim plan" was issued, setting a deadline of November 2005 for the final plan. According to the GAO, the interim plan was incomplete: *it lacked both national-level milestones and sector-specific security plans.*

The plan remains incomplete to this day. We can't even get proposals ready in a timely matter. This is unconscionable.

I'm also seriously concerned that the Department is not devoting enough manpower to this threat. According to an August 12th response by DHS to a request made by committee staff, there was only one full time employee staffed exclusively to control system projects at the National Cyber Security Division in the department.

One person. Surely it takes more than a single, lonely individual to effectively coordinate the public and private efforts in the control systems field?

The fact is this: the threats and dangers to control systems are increasing.

Standardized technologies currently being used have commonly known vulnerabilities allowing for easy exploitation. The connectivity of control systems to other networks offers additional beaches in security. Widespread public availability of technical information about control systems continues to present a serious risk.

And the federal government isn't ready.

I look forward to the testimony from our witnesses today, and I hope that this hearing is the first in a series of actions our committee takes to ensure that control systems are as safe as they possibly can be.

Mr. LUNGREN. All Members are reminded that opening statements may be submitted for the record.

[The information follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE PETER KING

Thank you. And thanks to our witnesses for appearing before these Subcommittees today.

As Chairman Lungren pointed out-SCADA systems are an integral part of our critical infrastructure. These real time control systems operate our major industries that we rely on everyday, including our gas, water, electric and oil facilities. They are integral parts of our efficient operation of these industries- and our National economy. SCADA systems control integral and vital processes of our infrastructure with potential significant physical and public health and ramifications if they are shut down or misused. SCADA systems are part of the larger issue of cybersecurity and a vital component of critical infrastructure protection.

Because these systems are connected to the internet or our telephone network—these systems can be remotely accessed, and they are easily penetrated. These systems were created decades ago and were designed before security was as great a concern as it is now. Many systems are not protected by basic security features, such as passwords or firewalls.

The good news is that there have been no reported terrorist cyber-attacks on domestic critical infrastructure control systems that have resulted in significant dam-

age. This does not indicate that it is not possible or that terrorists are not interested in these vulnerabilities. There are reports that al-Qa'ida computers found in Afghanistan contained information on structural analysis programs for dams and that these computers were used to search for information on SCADA systems specifically.

There have been cases of non-terrorist individuals breaking into control systems and in some cases causing damage including an instance in Australia, in 2000 where a malicious former employee remotely accessed the control system of a sewage plant and discharged almost 265,000 gallons of sewage into the local environment.

There are two things that we need to see happen. We need to be working with industry and the National Labs to develop new secure systems that can be put in as replacements or for new industries. But we can not expect all of the owners and operators of SCADA systems to incur the expensive cost of replacing existing control systems. Rather, the second thing we need to see- is procedures and protocols developed and distributed that can improve the security of these critical systems. Utilizing encryption, installing security software on outdated systems, training and educating employees on basic security procedures, these things can be done to reduce the vulnerabilities without entirely replacing the systems themselves.

I look forward to hearing from this panel on their thoughts on these issues and what they have done specifically to improve the security of the existing SCADA systems and the new SCADA systems being produced. I know that DHS has worked with the National Labs and the Dept. of Energy to develop programs to test existing systems, to model interdependencies and vulnerabilities—but it is also evident that the private sector has not waited for the Federal government to provide guidance. I look forward to hearing from our private sector witnesses as well, as to their efforts to secure this vital component of our National infrastructure.

Thank you again, and I look forward to your testimony and the opportunity to ask you questions.

PREPARED OPENING STATEMENT OF THE HONORABLE BENNIE G. THOMPSON

Thank you Mr. Chairman, Ranking Member Sanchez. I am glad we are here today to consider this important issue.

SCADA systems perform vital functions in running much of our industrial and critical infrastructure processes.

As technology continues to develop, this country will become more reliant on computerized control systems to perform these vital monitoring functions.

It is imperative that the Congress and this Administration act quickly to solve the serious security problems that plague SCADA and control systems.

The possibilities of a terrorist breaching a SCADA system are incredibly frightening.

Nuclear power plants—like the one located in Port Gibson, Mississippi, in my District—can potentially be at risk.

Electric grids, water management systems, and oil and gas control systems are also all at risk. Attacks can result in unquantifiable losses of infrastructure, money, and lives.

The risks to control systems posed by a natural disaster, like Hurricane Katrina, must also be considered.

The hurricane shut down the electrical grid along the Gulf Coast, thereby forcing two critical pipelines to shut down.

We're all still paying at the gas pump partially because of that failure.

we spent the time, money, and energy building our critical infrastructure systems; we must now spend the time, money, and energy to protect them.

As you all know, protecting SCADA and control systems requires a commitment from two entities.

The private sector must continue to identify current security risks, modify and adopt new encryption standards, and create new technologies to secure future systems.

It's also important for us here in Congress to determine what role the federal government should play.

Should we provide incentives for SCADA systems to comply with best practices? Should we establish new guidelines for existing SCADA systems?

Should we use the leverage the federal government has when buying SCADA systems for itself in order to create changes across the market, as Mr. Paller will testify about today?

In terms of current federal efforts, I am particularly concerned about what the National Cyber Security Division at DHS is doing right now.

I am glad that the director of the NCSD is here today to answer some of those questions. Mr. Purdy, for example, I also want to hear more about what the NCSD is doing to help DHS complete the cyber security portions of the National Infrastructure Protection Plan. A final version of the NIPP was due last December. we are still waiting for it.

I look forward to hearing from the members of this panel on all of these issues. Thank you Mr. Chairman.

Mr. LUNGREN. We are pleased to have a distinguished panel of witnesses before us today on this important topic. The Chair would recognize Mr. Donald "Andy" Purdy, the Acting Director of the National Cyber Security Division of the U.S. Department of Homeland Security, to testify.

I would just mention to all of you we are under the gun, I am sorry about that, because of votes that we are going to have. I would ask you to please restrict your oral statements to 5-minutes, and your prepared statements will be made a part of the record.

STATEMENT OF DONALD "ANDY" PURDY, ACTING DIRECTOR, NATIONAL CYBER SECURITY DIVISION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PURDY. Good afternoon, Chairman Lungren and distinguished members of the committee. My name is Andy Purdy. I am the Acting Director of the Department of Homeland Security's National Cyber Security Division. I am pleased to appear before you today to share with you the work of NCSD to address one of the significant threats to our cyberspace and critical infrastructure, industrial control systems. In my testimony today I will focus on our Control Systems Security Program.

To carry out our mission and related responsibilities under the National Infrastructure Protection Plan, we have identified two overarching priorities: to build an effective national cyberspace response system and implement a cyber risk management program for critical infrastructure protection of which our control systems effort is an important risk mitigation effort.

The interdependency between physical and cyber infrastructures is particularly acute in the use of control systems as integral operating components by many of our critical infrastructures. To assure immediate attention is directed to protect these systems, we have established a Control Systems Security Program to coordinate efforts among Federal, State and local governments, as well as control systems owners, operators and vendors, to improve control system security within and across all critical infrastructure sectors. As a key component of the program, in August, 2004, we established a U.S. Computer Emergency Readiness Team Control Systems Security Center in partnership with Idaho and Sandia National Laboratories and other Department of Energy national laboratories. The center's mission is to reduce the risk of cyberattacks on control systems, and it partners with control systems industry associations, universities, vendors and industry experts.

Our program encompasses five goals. First we seek to enhance the US–CERT capabilities for control systems security to coordinate incident management, provide timely situational awareness information, assess vulnerabilities, encourage voluntary reporting and manage vulnerability and threat reduction activities.

Our second goal is to reduce control system cyber vulnerabilities in critical infrastructure. We have developed the draft protection framework for identifying protection measures and comparing them against existing security standards. In addition, the framework includes a self-assessment tool developed to allow owners and operators to perform on-site assessments against the database of categorized security requirements. We will soon pilot the tool with multiple infrastructure sectors and will assist selected control systems owners and operators in using the tool at their sites.

Our third goal is to bridge industry and governmental efforts through participation in working groups, standards development bodies and user conferences. In partnership with the Department of Homeland Security Science and Technology Directorate, we chair the Process Control System Forum, which includes industry, academia and government representatives. It is designed to accelerate the development of technology that will enhance the security, safety and reliability of control systems, including legacy installations.

Our fourth goal is to develop control systems security awareness and create a self-sustaining security culture within the control systems community. A key element is our awareness workshop program, which we began in May of this year and will have completed approximately eight workshops by the end of this year.

Our final goal is to make strategic recommendations for improvements to future generation secure control systems and security products. We have responsibility for developing requirements for cybersecurity R&D projects to inform our Science and Technology Directorate's research priorities, and we coordinate with S&T in the development of new technologies for securing control systems and networks.

We have a robust effort underway with our partners to address the security of control systems through our Control System Security Program. The efforts of our center toward realizing the program goals has moved the ball forward in this arena by increasing the control systems communities' awareness of the need for cybersecurity and helping to provide them the tools and resources to secure their control systems. We continue to further these strategic goals through advancement of our key initiatives.

We are committed to achieving success in meeting our goals and objectives, but we recognize we cannot do it alone. We will continue to meet and work with industry representatives, our government counterparts, academia and State and local government to formulate and enhance partnerships needed for productive collaboration, and leverage the efforts of all so we as a Nation are more secure in cyberspace and in our critical infrastructure.

Again, thank you for the opportunity to testify to you today, and I look forward to answering your questions.

Mr. LUNGREN. Thank you very much, Mr. Purdy.

[The statement of Mr. Purdy follows:]

PREPARED STATEMENT OF DONALD (ANDY) PURDY, JR.

Good morning Chairman King and distinguished members of the Committee. My name is Andy Purdy, and I am the Acting Director of the Department of Homeland Security's National Cyber Security Division (NCSD). I am delighted to appear before you today to share with you the work of the NCSD to address one of the significant threats to our cyberspace and critical infrastructure—industrial control systems.

In my testimony today, I will provide an overview of NCSD's mission and goals, priorities, and partnerships, with a particular focus on our Control Systems Security Program. The Control Systems Security Program addresses the cyber security of industrial control systems that run the operational processes within the nation's critical infrastructure.

DHS and Critical Infrastructure Protection

Over the course of the past several months Secretary Chertoff conducted a systematic evaluation of the Department's operations. On July 13th, Secretary Chertoff announced the results of that evaluation and outlined his six point agenda for the path ahead for the Department. As part of this agenda, the Secretary announced several Departmental organizational changes. Among these was the creation of a new Preparedness Directorate which would house a newly created office of the Assistant Secretary for Cyber Security and Telecommunications. According to Secretary Chertoff, "Securing our cyber systems is critical not only to ensure a way of life to which we've grown accustomed, but more importantly to protect the vast infrastructure these systems support and operate."

Currently, the Office of Infrastructure Protection (IP), located within the Information Analysis and Infrastructure Protection (IAIP) Directorate, is responsible for all critical infrastructure and key resource protection. The Office of Infrastructure Protection has four component divisions: (1) the Infrastructure Coordination Division (ICD), (2) the Protective Security Division (PSD), (3) the National Communications System (NCS), and (4) the National Cyber Security Division (NCSD).

In December 2003, President Bush issued Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD–7), which established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Among other things, HSPD–7 identified seventeen (17)[1] critical infrastructure and key resource sectors and assigned responsibility for each to a Sector Specific Agency (SSA), with DHS serving as the overall program coordinator.

Additionally, HSPD–7 set forth how DHS should address critical infrastructure protection, including development of a "summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources."[2] To meet this mandate, IP developed the interim National Infrastructure Protection Plan (NIPP), a plan that is to serve as the guide for addressing critical infrastructure and key resource protection. It sets forth a risk management framework for public and private sector stakeholders to work together to identify, prioritize, and conduct vulnerability assessments of critical assets and key resources in each sector. It also includes the identification of interdependencies of critical assets and key resources both within and across the sectors as well as providing priority protective measures that owners and operators of such assets should undertake to secure them. Recognizing that more that 85 percent of the critical infrastructure is owned and operated by the private sector and that the development of public-private partnership is paramount to securing our nation's assets, private sector-led Sector Coordinating Councils (SCCs) are being established to work with their appropriate SSA via Government Coordinating Councils (GCC), which represent the government agencies that have a role in protecting the respective sectors.

Currently, the Office of Infrastructure Protection is finalizing the NIPP and it is expected to be released later this year. This finalized document will refine the public-private partnership model and a process for protecting our critical infrastructures from physical or cyber attack or natural disasters.

DHS and Cyber Security

In June 2003, in response to the President's National Strategy to Secure Cyberspace, the Department of Homeland Security created the NCSD as a national focal point for cyber security. The national strategy established the following five national priorities for securing cyberspace:

Priority I:A National Cyberspace Security Response System

---

[1] The NIPP identifies the following Critical Infrastructure Sectors and Key Resources: Food and Agriculture; Public Health and Healthcare; Drinking Water and Wastewater; Energy; Banking and Finance; National Monuments and Icons; Defense Industrial Base; Information Technology; Telecommunications; Chemical; Transportation Systems; Emergency Services; Postal and Shipping; Dams; Government Facilities; Commercial Facilities; Nuclear Reactors, Materials, and Waste.

[2] Homeland Security Presidential Directive 7, December 17, 2003; http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III: A National Cyberspace Security Awareness and Training Program
Priority IV: Securing Government'S Cyberspace
Priority V: National Security and International Cyberspace Security Cooperation

Given today's interconnected environment and DHS's integrated risk-based approach to critical infrastructure protection, NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To meet that mission, NCSD developed a Strategic Plan that establishes a set of goals with specific objectives for each goal, and milestones associated with each objective. The Strategic Plan goals, which are closely aligned with the Strategy, HSPD–7, the NIPP, and the Cyber Annex to the recently announced National Response Plan, are as follows:

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents;
2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks;
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace;
4. Foster adequate training and education programs to support the Nation's cyber security needs;
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

To meet these goals, NCSD is organized into four operating branches to address the various aspects of the risk management structure: (1) U.S. Computer Emergency Readiness Team (US-CERT) Operations to manage the 24x7 threat watch, warning, and response capability that can identify emerging threats and vulnerabilities and coordinate responses to major cyber incidents; (2) Strategic Initiatives to manage activities to advance cyber security in critical infrastructure protection, control systems security, software development, training and education, exercises, and standards and best practices; (3) Outreach and Awareness to manage outreach, cyber security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders; and (4) Law Enforcement and Intelligence to coordinate with and share information between these communities and NCSD's other constituents in the private sector, public sector, academia, and others, and also to coordinate DHS efforts within interagency response and mitigation of cyber security incidents. Together, these branches make up NCSD's framework to address the cyber security challenges across our key stakeholder groups and build communications, collaboration, and awareness to further our collective capabilities to detect, recognize, attribute, respond to, mitigate, and reconstitute after cyber attacks.

The Strategy, HSPD–7, and the interim NIPP provide NCSD with a clear operating mission and national coordination responsibility. To carry out this mission and its related responsibilities, NCSD has identified two overarching priorities: to build an effective national cyberspace response system and to implement a cyber risk management program for critical infrastructure protection. Our focus on these two priorities and related programs addresses the overarching NIPP Risk Management methodology and establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

Within the second priority, in addition to fulfilling our NIPP role as the Sector Specific Agency for the Information Technology (IT) Sector and providing cross-sector cyber security guidance to all sectors, NCSD undertakes a cyber risk mitigation approach focused on three key areas. These include the Internet Disruption Working Group, the Software Assurance Program, and the Control Systems Security Program.

NCSD and Control Systems Cyber Security

The interdependency between physical and cyber infrastructures is hardly more acute than in the use of control systems as integral operating components by many of our critical infrastructures. "Control Systems" is a generic term applied to hardware, firmware, communications, and software used to perform vital monitoring and controlling functions of sensitive processes and enable automation of physical systems. Specific types of control systems include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

Examples of the critical infrastructure processes and functions that control systems monitor and control include energy transmission and distribution, pipelines, water and pumping stations, telecommunications, chemical processing, pharmaceutical production, rail and light rail, manufacturing, and food production. Increasingly, these control systems are implemented with remote access and connections to open networks such as corporate intranets and the Internet. Older control systems that operated with manual components, vacuum actuators, and proprietary software are rapidly being upgraded with modern computer systems. These sophisticated IT tools are making our critical infrastructure assets more automated, more productive, more efficient, and more innovative, but they also may expose many of those physical assets to physical consequences from new, cyber-related threats and vulnerabilities.

Control systems represent an attractive target for malicious actors for several reasons. First, they provide a possible avenue for inflicting physical, environmental, or economic harm to the nation from a distance. Second, relatively mature attacking tools have been developed and are available on the Internet. Finally, these tools can be used with little technical expertise to attack control systems that are accessible from the Internet.

To assure immediate attention is directed to protect these systems, NCSD established the Control Systems Security Program to coordinate efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors.

The Program incorporates five highly integrated goals to address the issues and challenges associated with control systems security.

1. Coordinate control system incident management, provide timely situational awareness information for control systems, assess control system vulnerabilities, encourage voluntary reporting, and manage control system vulnerability and threat reduction activities by enhancing the US-CERT's capabilities for control systems security;
2. Reduce control system cyber vulnerabilities in Critical Infrastructure by establishing a proactive environment for risk reduction and security assessments, to evaluate systems, and to work with control systems owner/operators and vendors to resolve vulnerabilities;
3. Bridge industry and governmental efforts through participation in working groups, standards development bodies, and user conferences to build cooperative and trusted relationships and enhance control systems security efforts;
4. Develop control systems security awareness and create a self-sustaining security culture within the control systems community; and
5. Make strategic recommendations as to the funding, development, and testing of next-generation secure control systems and security products.

Goal 1—Enhance US-CERT capabilities for control systems cyber security

Our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents and vulnerabilities, and mitigation of threat actions specific to critical control systems functions. NCSD established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other Department of Energy (DOE) National Laboratories[3] in August, 2004. Through the use of Cooperative Research and Development Agreements (CRADA's) and other mutually benefiting agreements, the CSSC also incorporates partners from control systems industry associations, universities, vendors, and industry experts. The CSSC mission is to reduce the risk of cyber attacks on control systems, and as such, it provides facilities and expertise to support the reduction of risk in critical infrastructure through site and system assessments, demonstrations for education and awareness, risk assessment and risk analysis, adversarial awareness, and coordination among the national laboratories.

Through its partnerships and technological improvement efforts for systems and facilities, the CSSC has been maturing response capabilities to support US-CERT with control system expertise. The CSSC continues to work with the US-CERT in enhancing their ability to provide initial control system guidance and expertise, and a CSSC limited access secure portal (*https://us-cert.esportals.net/*) has been established for information coordination and dissemination of cyber threat and vulnerability alerts. A web site is under development to share control systems security information with our cyber security partners and the control systems community. The

[1] Pacific Northwest, Los Alamos, Argonne, Sandia, Lawrence Livermore and Savannah River

web site, which will be available in FY06, will also provide information, resources, and links for owners and operators to effectively defend their control systems. A "Tier II" support function will further support US-CERT by leveraging CSSC partners in incident response and vulnerability handling, and performing in-depth evaluation of specific attacks or exploits and determining the impact on various operating systems, components, and vendor systems.

In FY06, CSSC will explore the need for establishing a trusted third-party within academia to serve as a voluntary reporting center to encourage open communication among the private sector regarding emerging control system threats and exploits. As such, the CSSC is developing a control systems incident management support tool to enhance US-CERT cyber threat notification efforts. It is designed for use when a new vulnerability is detected and will enable the identification of critical infrastructure at greatest risk to an identified threat, thereby enabling the CSSC to rapidly notify the facilities at the greatest risk. Owners and operators can then implement protective measures as appropriate to reduce that risk and mitigate damage to their systems. It is important to note that the effectiveness of the tool is dependent on the acquisition of current owner/operator system data. NCSD continues to work with Sector Specific Agencies to obtain data from the various sectors necessary to utilize the tool and maximize its benefits.

Goal 2—Reduce control system vulnerabilities in critical infrastructure

To reduce control system vulnerabilities in our critical infrastructure, CSSC developed a draft cyber security protection framework for identifying control systems security protection measures and comparing them against existing security standards. The cyber security protection framework, which is based on the Common Criteria and an Industrial Control System Security Protection Profile developed by the National Institute of Standards and Technology, supports NCSD's mission to reduce cyber security risk within control systems. The framework provides a systematic methodology for assessing the cyber security posture of control systems. It is designed to reduce the burden on owners and operators by providing them with a means to select protective measures that apply to their specific architecture and operating environment and reduce their respective risk.

Application of the framework methodology results in a risk-based set of security measures. Risk is defined by DHS as **Risk = Threat x Vulnerability x Consequence.** To calculate quantitative values for risk, one must define the system of interest, establish attack-defense-failure scenarios, and consider the consequences of a successful attack. Then, protection measures are identified to reduce risk. The overall goal is to provide a quantitative, traceable, and supportable value of risk.

As part of this framework, the CSSC also has capabilities at INL to perform vulnerability assessments of control systems. For example, the CSSC leverages the National SCADA Test Bed funded by DOE and operated in partnership with Sandia National Laboratories. Linkages with these test beds and assessment facilities provides the CSSC with incoming and outgoing data traffic and communication channels necessary for the replication of control systems (e.g., PCS, SCADA) and components. These testing capabilities also support quick mock-ups of control systems and/or components to evaluate existing threats, vulnerabilities, and incidents as they are reported to the US-CERT.

The CSSC utilizes a unique "plug and play" patching system that allows engineers to assess systems or components in an environment simulating the conditions found in industry to include multiple communication pathways and live incoming and outgoing control systems specific data traffic. This allows for in-depth assessments of control systems in a near true-to-life environment. The CSSC is working with commercial vendors and DOE to complete assessments of three different control systems to identify cyber vulnerabilities, reverse engineer exploits, and provide solutions to secure vendor systems. A code-based analysis has also been conducted in cooperation with a vendor/manufacturer to identify possible vulnerabilities and recommendations to secure the system.

Our adversaries are developing tools to hack into and take over control systems, and we need greater collective awareness of those capabilities to understand specific threats to and vulnerabilities of our control systems. As such, CSSC tracks information on current control systems security trends and threats, review and assesses new vulnerabilities and exploits as they are discovered or reported, and conducts analysis to better understand adversarial tools and capabilities. The CSSC considers specific exploit assessment scenarios on control systems and "reverse engineers" exploits to provide solutions to industry before an exploit is made public.

The cyber security protection framework also leverages best practices from industry for securing control systems against cyber attacks and organizes them so the control systems community can identify specific solutions to their security

vulnerabilities. As part of the framework, implementation tools, such as a "self-assessment tool," have also been developed to allow owners and operators of industrial control systems to perform on-site self-assessments against a database of categorized security requirements. Each security requirement is supported by recommendations for meeting the requirement and mitigating vulnerabilities within the architecture of that particular control system. As new vulnerabilities emerge and associated solutions are developed, the framework of security requirements will expand and new protection solutions will be made available to the control system community. The protection framework provides categorized and graded guidance, component by component, for improving cyber security of control systems.

The draft security protection framework and its associated implementation tools are ready for validation. NCSD will soon pilot the self-assessment tool with multiple infrastructure sectors and will assist selected control system owners and operators in using the tool at their sites. This effort will help owners and operators identify security vulnerabilities within their systems, recommend solutions for reducing the risk of successful cyber attacks, and prioritize risk reduction efforts. The pilot effort will also allow NCSD to validate and enhance the self-assessment tool for future, widespread roll-out across the control system community. NCSD is also working with PSD and other Sector Specific Agencies to ensure that concepts from the cyber security protection framework are integrated into risk and vulnerability assessments across the sectors. For example, NCSD is working closely with the American Society of Mechanical Engineers and PSD to incorporate cyber into the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework.

Goal 3—Bridge industry and governmental efforts through participation in working groups, standards development bodies, and user conferences

A primary objective of NCSD's Control Systems Security Program is to coordinate efforts among Federal, State, and local governments, as well as control system owners, operators, and vendors to improve control systems security within and across all critical infrastructure sectors.

In partnership with DHS' Science and Technology (S&T) Directorate, NCSD chairs the Process Control System Forum (PCSF). The PCSF includes industry, academia, and government representatives and is designed to accelerate the development of technology that will enhance the security, safety, and reliability of control systems, including legacy installations.

In addition to the PCSF, the CSSC works to enhance private sector awareness through participation in industry association meetings, user groups, and standards coordination work groups. For example, most recently, representatives from CSSC participated in a Railroad Association meeting in Annapolis, Maryland, the Pacific Northwest Economic Region 15th Summit, and the Interagency Forum for Infrastructure Protection in Portland, Washington. At all of these gatherings, attendees were provided with an overview of the CSSC program, capabilities, and with information on how they can participate and take advantage of what the CSSC program has to offer, including alert and informational bulletins, self-assessment and risk reduction calculation tools.

CSSC has also established relationships with a number of industry partners, including partnerships designed to facilitate initial assessments and develop risk reduction plans in various industry sectors. Our private industry partners provide experience in understanding vulnerabilities and operational perspectives, and bring established contacts within the control systems community. Specifically, they provide CSSC with control system expertise from various critical infrastructure sector perspectives; expertise and feedback on assessment tools; subject matter expertise regarding development of security requirements and best practices; assessment, research, and risk assessment capabilities; and contacts and opportunities to interface with sectors.

CSSC is also working with control system vendors to provide equipment for assessments to be conducted at CSSC facilities. They assist in identifying vulnerabilities based on their experience and work to resolve vulnerabilities in next generation and legacy systems as a result of assessments performed against their systems. A number of industries (e.g., oil and gas, chemical, petro-chemical, electrical, power generation plant automation [coal, hydro, and gas fired plants], and transportation) are contributing to these CSSC efforts to reduce cyber vulnerabilities in control systems. Partnerships with members of the control system community are designed to help NCSD better assist owners and operators secure their systems.

Goal 4—Enhance control systems security awareness

The NCSD is engaged in several activities designed to increases awareness and provide the tools and products necessary to enable the critical infrastructures and

key resources to secure their control systems against cyber threats. A key element is CSSC's awareness workshop program.

Our "threat-brief, demonstration, and mitigations" workshop has been well received by the control systems community. The first workshop was held in May, 2005 at a PCSF meeting in Dallas, Texas. Since then additional workshops have been held in Bellevue, Washington and Idaho Falls, Idaho. We anticipate that by late 2005, approximately eight workshops will have been conducted. The workshops include a brief overview of the threat picture, a cyber vulnerability demonstration, and a discussion of mitigation steps. NCSD has found that cyber vulnerability demonstrations are an effective method to show the impact that cyber attacks can have on their control systems and operations and that cyber security is essential to protect them.

Goal 5—Make strategic recommendations for improvements to future generation secure control systems and security products

Cyber-related research and development (R&D) is vital to improving the resiliency of the Nation's critical infrastructures. This difficult strategic challenge requires a coordinated and focused effort from across the Federal Government, State and local governments, the private sector, and academia to advance the security of critical cyber systems.

Two components within DHS share responsibility for cyber R&D. The Science & Technology (S&T) Directorate serves as the primary agent responsible for executing cyber security R&D programs. NCSD has responsibility for developing requirements for cyber security R&D projects. NCSD supports the overall DHS R&D mission by identifying areas for cyber innovation and coordinating with S&T. NCSD collects, develops, and submits cyber security R&D requirements to provide input to the federal cyber security R&D community and specifically to inform the DHS S&T Directorate's cyber security research priorities. NCSD coordinates with S&T on the development of new technologies for securing SCADA systems and networks.

NCSD's Control Systems Security Program identifies R&D cyber security requirements for legacy and next generation control systems and security products through US-CERT CSSC operational activities such as incident management, site and system assessments, and analyses. As difficult problems which would benefit from advanced technological solutions are discovered, requirements are identified and forwarded to control systems vendors and DHS S&T for new R&D projects. Best practices, common vulnerabilities, and requirements for security standards are also shared with the control systems community to promote enhanced security for legacy and new control systems.

DHS S&T manages the Congressionally directed funding for the Institute for Information Infrastructure Protection (I3P). The I3P is a national research consortium composed of more than two dozen research entities, including academic institutions, non-profits, federally funded labs, and FFRDCs. In early 2005, the I3P launched a major initiative focused on addressing the vulnerabilities of SCADA systems in the oil and gas industry.

Moving Forward

NCSD has a robust effort underway to address the security of control systems through our Control Systems Security Program. The efforts of the CSSC toward realizing the five goals the Program sets forth, including the enhancement of capabilities, initiatives to reduce vulnerabilities, and establishment of partnerships, has moved the ball forward in this arena by increasing the control system communities' awareness of the need for control systems cyber security and providing them the tools and resources to secure their control systems.

Many activities are planned for the near future including:

- Developing and finalizing the CSSC portal and web site to enhance capabilities and encourage greater information exchange with the control system community.
- Supporting vulnerability assessments to determine the cyber security posture of legacy and next generation control systems at critical sites. Assessments will identify critical components threat vectors, and misconfigurations in hardware, applications, and network topologies within our current infrastructure and recommend protective measures. This information will aid in determining the level of compliance with current best practices and control system protection framework requirements.
- Continuing to integrate CSSC activities, skills, and capabilities to identify particular high risk cyber vulnerabilities. Specifically, for FY06 high-risk system vulnerabilities will be identified in at least two critical infrastructure sectors and then security enhancements to mitigate those vulnerabilities will be

identified. Other site assessments will be supported as appropriate to identify cyber risks to control systems.

• Encouraging the voluntary implementation of security measures. The CSSC will accomplish this through development of a "Business Case," beginning in FY06. Development of a business case will demonstrate cost-benefit where the cost will be represented as the cost of implementing countermeasures and benefit will be the reduction of risk. Risk analysis is the basis for the business case.

• Continuing to work with PSD and other Sector Specific Agencies to integrate cyber security and control systems security efforts into risk and vulnerability assessment efforts such as Comprehensive Reviews, the Vulnerability Identification Self Assessment Tool, and the Risk Analysis and Management for Critical Asset Protection.

• Continuing to participate in forums and meetings to raise awareness while conducting targeted outreach activities in sectors and with senior executives to not only pilot and validate our control systems protection framework and tools but also to create an understanding among control system owners and operators of the need for and importance of security.

We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts, academia, and state and local representatives to formulate the partnerships needed for productive collaboration and leverage the efforts of all, so we, as a nation, are more secure in cyberspace and in our critical infrastructures.

Again, thank you for the opportunity to testify before you today. I would be happy to answer any questions you have.

Mr. LUNGREN. The Chair would now recognize Mr. Larry Todd, the Director of Security, Safety and Law Enforcement for the Bureau of Reclamation, U.S. Department of Interior, to testify.

STATEMENT OF LARRY TODD, DIRECTOR OF SECURITY, SAFETY AND LAW ENFORCEMENT, BUREAU OF RECLAMATION, U.S. DEPARTMENT OF THE INTERIOR

Mr. TODD. Thank you, Mr. Chairman and distinguished members of the subcommittee. I am pleased to appear before you today to tell you about the security of the control systems used by the Bureau of Reclamation.

Reclamation uses SCADA systems as tools to enable us to meet our mission of water delivery, power generation, flow monitoring and water regulation. SCADA is used to control outlet works, valves at dams, to control hydroelectric generators and associated circuit breaker switches and transformers, and to control pumps and gates on water delivery systems and canals. However, we do not use SCADA controls to operate the spillway gates, nor for flood control operations.

Reclamation has a number of security features built into the SCADA operation. For instance, no SCADA system is attached to the Internet, and therefore, the systems cannot be accessed by the Internet. There are software controls within SCADA systems to protect against unauthorized operation, and on some facilities we have mechanical controls that prevent operation beyond set parameters. In addition, Reclamation regularly tests to ensure the connectivity does not exist.

To help identify physical and cyber vulnerabilities, Reclamation uses independent organizations to evaluate our security posture. We have had numerous investigations by the Inspector General's Office, and they report that the SCADA systems are operating in relative safety from potential catastrophic cybersecurity threats.

In summary, Reclamation recognizes that SCADA plays a key role in protecting critical infrastructure components. Where we em-

ploy SCADA systems, we believe we have taken responsible steps to ensure their security and safe operation. We also will employ better assessment and protection tools as they become available.

Thank you for this opportunity to describe Reclamation's use of SCADA. I would be pleased to answer any questions the committee may have.

Mr. LUNGREN. Thank you very much, Mr. Todd.

[The statement of Mr. Todd follows:]

PREPARED STATEMENT OF LARRY TODD

Mr. Chairman, my name is Larry Todd, and until recently I served as the Director of Security, Safety, and Law Enforcement for the U.S. Bureau of Reclamation. Established in 1902, Reclamation is known primarily for the dams, power plants, and canals we have built and operate in seventeen western States. Reclamation is our Nation's largest wholesaler of water, and its second largest producer of hydroelectric power. I am pleased to appear before you today to tell you about the security of the control systems used by the Bureau of Reclamation.

Reclamation's Supervisory Control and Data Acquisition (SCADA) Systems

Reclamation employs SCADA systems as tools to enable us to meet our mission obligations of providing essential services and commodities. These obligations include electric power generation, flood monitoring, water regulation, and water delivery. To accomplish these goals, Reclamation controls water release gates and valves at dams; hydroelectric generators, circuit breakers, switches and transformers at power plants; and pumps and gates on waterways and canals.

Reclamation's SCADA systems collect information about our facilities through transducers, converting information such as gate position, reservoir level, hydroelectric generator output, and water flow to electrical signals for processing in the SCADA system's computers. Once in the computers, the information is examined for any unusual characteristics, such as whether it exceeds an expected value. When information does not meet expectations, alarms may be triggered to inform operations staff of the situation, enabling them to take corrective actions. Reclamation's major SCADA control centers are manned at all times, enabling operations staff to react to both normal operations and emergency situations 24 hours a day and 365 days a year.

Along with collecting information, Reclamation's SCADA systems also facilitate our operations staff's reaction to normal and abnormal operational needs. They do this by supporting the supervised remote control of our facilities. By providing the operations staff with information about the facility, informed decisions can be made quickly and the appropriate actions taken. The SCADA systems computers help to supervise these decisions by ensuring that they meet safe operational criteria.

Protecting Reclamation's SCADA Systems

The focus of security efforts has changed since SCADA systems were first employed by Reclamation. In those early years SCADA design focused almost entirely on the operational integrity of the SCADA systems. In all cases where SCADA systems were permitted to control equipment, the safety and reliability of the control was examined and appropriate improvement measures were engineered and incorporated. This supported safer equipment operation and permitted the disabling of SCADA control if necessary. This was done to protect the equipment and to ensure the safety of the public and Reclamation personnel in the event of a SCADA malfunction. These safety measures acted independently from the SCADA system to ensure that the failure of the SCADA system did not adversely affect the safety measures. If the safety of SCADA control actions could not be ensured, additional steps were taken to limit the degree of SCADA control or the control was not enabled. Reclamation still follows these practices in implementing its SCADA systems, providing a significant measure of operation security for its SCADA controlled facilities.

From the very beginning of Reclamation's use of SCADA systems, we have maintained a policy of not connecting our SCADA systems to our administrative networks. Today we adhere to that policy in all but the most unusual of situations. All connections to SCADA systems are minimized. Reclamation does not connect its SCADA systems to the Internet and routinely tests to ensure that such connectivity does not exist. Wherever practical, connections to our SCADA systems do not use Internet-like protocols, instead employing simple, limited capability, serial protocols. Those connections that must be present and that use Internet-like protocols are protected by firewalls and intrusion detection systems. Reclamation has adopted "best

practices" and follows the cyber security guidance outlined by the National Institute of Standards and Technology (NIST) in their Special Publications.

In addition, Reclamation has evaluated and improved both personnel and physical security at our SCADA facilities. We perform background checks on key personnel and have "hardened" our facilities and control rooms through the addition of various access controls. This includes the access to our SCADA system control consoles.

To help identify physical and cyber vulnerabilities within the organization, Reclamation has invited independent organizations, including some represented by other panel members, to evaluate our security posture. We have also supported numerous investigations by our Inspector General's Office, some of which included limited penetration testing of our SCADA systems. The Inspector General's FY05 management report concluded that "the SCADA systems are operating in relative safety from potentially catastrophic cyber-security threats." To maintain these results, we are continuously evaluating and implementing prudent and practical security improvements.

Actions to Improve SCADA Security

Despite our security successes so far, Reclamation believes we can still take additional steps to improve the security of our SCADA systems. These steps, specifically identified and addressed in internal documents, will create more rigorous testing processes, improve and increase the frequency of security assurance reviews, and establish more comprehensive security planning targets. We also favor additional steps to improve the coordination of SCADA security efforts at both the Federal and private sector levels. Close coordination will assure consistency of Federal and private sector standards and security guidance, and could also help ensure that an appropriately rigorous security baseline is established for SCADA systems employed in different industry segments, depending on the significance of the infrastructure monitored or controlled.

In Summary

Reclamation recognizes that it plays a key role in protecting critical infrastructure components, including dams, waterways, water resources, and electrical generation capability. Where we employ SCADA systems to facilitate the control of these components, we believe we have taken responsible steps to ensure their security and safe operation. We recognize that cyber security, as it applies to both administrative and SCADA systems, requires continuous monitoring and diligence. We believe our security program meets the challenges of these requirements, but look forward to contributing to and employing better development, assessment, and protection tools and techniques as they become available.

Mr. LUNGREN. The Chair would now recognize Mr. Sam Varnado, the Director of Information Operations Center at the Sandia National Laboratory, to testify.

STATEMENT OF SAM VARNADO, DIRECTOR, INFORMATION OPERATIONS CENTER, SANDIA NATIONAL LABORATORY

Mr. VARNADO. Thank you, Mr. Chairman and distinguished members of this committee. I am Sam Varnado from Sandia National Laboratories, with laboratories in both California and New Mexico.

First let me applaud the work the committee is doing. It is very important to the well-being of our citizens and to the national security. I am pleased to be part of it.

Today we are going to discuss SCADA systems. We are concerned about these systems. We are very worried about them because successful cyberattacks on these systems could lead to serious consequences, which include loss of life, destruction of equipment that is hard to replace, environmental insult and economic loss.

Let me give you one example. Mr. Chairman, in June of 1982, a huge explosion occurred in the Siberian wilderness in the former Soviet Union. The yield was estimated at 3 kilotons in that explosion. In his book At the Abyss: An Insider's History of the Cold War, Thomas Reed attributes the monumental explosion and re-

sulting fire to a cyberattack on the SCADA system that controlled the Trans-Siberian pipeline. According to Mr. Reed, the pipeline software that ran the pumps, turbines and valve settings was programmed to produce pressures far beyond those acceptable to the pipeline joints and wells. He further states that the malevolent software in this case was what we call today a Trojan. It had been implanted in the host software by a foreign intelligence service. This episode illustrates the physical damage that can be created by attacking a cybersystem.

SCADA systems are the soft underbelly of our infrastructure protection strategy in this country. The older stand-alone legacy SCADA systems are highly vulnerable. Some of these vulnerabilities are listed in my written statement. But today the trend is to replace those older systems with control systems that use the Internet as the backbone. From a security standpoint, this will make matters worse for the following reasons: First, U.S. computer networks are under daily attack, and adversaries are becoming more sophisticated. We are seeing structured, well-resourced attacks that are designed to steal information or disrupt and/or deny processes. For example, the recent Super Slammer, which was a fast worm, infected 60 percent of DOD's NIPRNet computers in 8 minutes.

Improvements in attack methods, particularly by sophisticated threats such as terrorist and nation states, are outpacing our activities in defensive countermeasures. The contest between the attackers and the defenders is a dreadful mismatch with the advantage strongly in the attacker's corner.

Second, information technology vendors release on average four new vulnerabilities each day at the same time new attack methods are proliferating.

Third, we have no alternative to the use of commercial off-the-shelf, or COTS, products in our information systems because of cost issues; therefore, most of the hardware and software we use is manufactured in countries whose interests do not always align with those of the United States. We are buying and embedding these products in very complex systems that we expect to be secure. We are essentially trying to build trusted systems from untrusted components, and many of us wonder if it can be done at all.

Fourth, most of the current emphasis in cybersecurity is on responding to hacker attacks that exploit the inherent vulnerabilities that are present in all networked computer systems. This effort is necessary and useful and should be increased, but a longer-term view is needed. We need to put more emphasis on addressing enterprisewide solutions and threats from the more sophisticated adversaries.

My suggestions for addressing these problems are as follows: First, reaffirm the concept of public/private partnerships, and encourage stronger collaboration among government, industry, universities and national labs. We need to put more effort into sharing information on threats, vulnerabilities, consequences of outages, training and technology.

Second, extend these partnerships to include helping the infrastructure owners make the business case for their investments in security upgrades.

Third, increase funding for cybersecurity technology to address the new threat and vulnerability environment and to keep the defensive efforts on par with the attack development activities being conducted by our adversaries.

Fourth, establish and fully fund a concentrated effort to provide defense against the sophisticated threat.

Finally, support the initiatives, directives and plans described in several reports that DHS and the administration have produced over the last few years.

Thank you, Mr. Chairman and members of the committee, for the opportunity to address you today. I would be happy to answer questions at the appropriate time.

Mr. LUNGREN. Thank you, Doctor.

[The statement of Mr. Varnado follows:]

PREPARED STATEMENT OF DR. SAMUEL G. VARNADO

Introduction

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify on the vulnerabilities of, and threats to, Supervisory Control and Data Acquisition (SCADA) systems. I am Dr. Sam Varnado, Director of Sandia National Laboratories' Information Operations Center. I have more than thirty years of experience in energy, information, and infrastructure systems development. I currently coordinate Sandia's activities in cyber security technology development, with special emphasis on critical infrastructure protection applications.

Sandia National Laboratories is managed and operated for the National Nuclear Security Administration (NNSA) of the U.S. Department of Energy (DOE) by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation. Sandia's unique role in the nation's nuclear weapons program is the design, development, qualification, and certification of nearly all the nonnuclear subsystems of nuclear warheads. We perform substantial work in programs closely related to nuclear weapons—including intelligence, non-proliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also conducts research and development for other federal agencies when our special capabilities can make significant contributions.

My statement will describe SCADA systems, identify some of the threats they face, describe some of the cyber vulnerabilities of these systems, discuss the consequences of disruptions, and explain Sandia's contributions and capabilities in SCADA system security. I will also comment on the gaps in current approaches to the problem, possible solutions, and needs that Congress might choose to address.

What Are SCADA Systems and How Are They Used in Critical Infrastructure Applications?

Both the national security of the United States and the well being of our citizens are highly dependent on the reliable operation of the nation's critical infrastructures. These infrastructures include electric power, oil and gas, banking and finance, transportation, telecommunications, and other networks. The operation of most of these infrastructures is controlled by SCADA systems. These systems are highly vulnerable to a wide range of threats, including terrorism. As an example, we have shown that it is possible to turn out the lights in most major U.S. cities through cyber attacks on SCADA systems. Disruption of these systems by any means will result in substantial economic loss, potential loss of life, long recovery times, and severe disruption of the lives of our citizens.

We should note that we use the term "SCADA" to include all real-time digital control systems, process control systems, and other related technologies. The control processes for each infrastructure are automated systems that combine humans, computers, communications, and procedures. Automated systems are used to increase the efficiency of process control by replacing high-cost personnel with lower cost computer systems. The widespread use of SCADA systems makes them critical to the safe, reliable, and efficient operation of physical processes common to most infrastructures.

High Level SCADA Vulnerabilities

SCADA systems have generally been designed and installed with little attention to security. Terrorist groups are aware of this. As noted in an article in the June 27, 2002 *Washington Post,* these systems have been targeted by al-Qa'ida terrorists. Some government experts have concluded that the terrorists hope to use the Internet as an instrument of bloodshed by attacking the juncture of cyber systems and the physical systems they control. The article further postulated that combined cyber and physical attacks could produce nightmarish consequences.

Sandia has been investigating vulnerabilities in SCADA systems for over ten years. During this time, many have been found. Our red team assessments show that security implementations are, in many cases, nonexistent or poorly implemented. Many of the older SCADA systems are operated in a stand-alone mode; that is, they are not connected to the Internet or to other corporate systems. Even so, these legacy systems have vulnerabilities, including inadequate password policies and security administration, no data protection mechanisms, and information links that are prone to snooping, interruption, and interception. When firewalls are used, they are sometimes not adequately configured, and there is often a "back-door" access because of connections to third-party contractors and maintenance staff. We have found many cases in which unprotected remote access allows users to circumvent the firewall. In addition, most of the SCADA manufacturers are foreign-owned.

In summary, it is easy for adversaries to take control of these legacy systems and cause disruptions with significant consequences. Today, the legacy systems are gradually being replaced by new SCADA systems that use the Internet as the control backbone. This change is being implemented to reduce cost and increase efficiency of operation. However, this trend substantially increases the possibility of disruptions because (1) the number of people having access to the system is substantially increased, (2) disruptions can be caused by hackers who have no training in control systems engineering, and (3) the use of the Internet exposes SCADA systems to all the inherent vulnerabilities of interconnected computer networks that are currently being exploited by hackers, organized crime, terrorists organizations, and nation states. Worms, viruses, network flooding, no-notice attacks through compromised routers, spyware, insider attacks, data exfiltration by outsiders who gain insider privileges (phishing), and Distributed Denial of Service attacks are all commonplace. Effectively combating these attacks requires increased awareness, new technology, and improved response and recovery capabilities.

Especially vulnerable is the electric power grid. Under restructuring, the grid is now being operated in a way for which it was never designed. More access to control systems is being granted to more users, the demand for real-time control has increased system complexity, and business and control systems are interconnected. In many cases, these new systems are not designed with security in mind. More vulnerabilities are being found, and the opportunities for disruptions are increasing rapidly. The complexity of the systems and the high degree of interdependency among the infrastructure sectors can lead to cascading failures in which failures in one sector can propagate to others.

Sandia has identified the vulnerabilities of SCADA systems and summarized them in a report—"Common Vulnerabilities in Critical Infrastructure Control Systems"—that is available from our Center for SCADA Security website (http://www.sandia.gov/scada). The report identifies the vulnerabilities that we uncovered in our red team assessments of systems in use by a diverse set of customers from the electric power, petroleum, natural gas, and water infrastructures. This document has been made available to other government agencies and to private industry.

SCADA Threats

Sandia performs vulnerability assessments using a red team process that models adversarial capabilities and approaches. It is essential to view SCADA systems from an adversarial perspective in order to identify their important vulnerabilities. We use adversarial modeling as a way of understanding threats from different political, social, and motivational structures so that relevant characteristics may be utilized to identify the classes of attacks that each adversary might be able to launch. Hackers, organized crime, cyber terrorists, and nation states are examples of different classes of adversaries with varying capabilities and attributes.

We consider two basic categories of adversaries: "outsiders" and "insiders." It is generally the goal of an outsider to acquire the attributes of an insider through such means as hijacking connections, password sniffing, and identity theft. Most U.S. critical infrastructure owners and operators have only a passing knowledge of the nature of the adversaries' capabilities. Consequently, the level of protection is low

and the probability of significant disruptions is high. Critical infrastructure owners and operators need to increase their awareness of both the vulnerabilities and the threat. They also need training in network defense, information about improvements in cyber security technology for control systems, and timely updates on threat information.

SCADA Attack Consequences

The consequences of disruptions to SCADA systems are numerous, expensive, and varied. Two examples are presented here simply to make the point that we must start thinking seriously about the security of SCADA systems.

In his book, *At the Abyss: An Insider's History of the Cold War,* Thomas C. Reed (former National Security Council member and Air Force Secretary) reported that in June 1982 the CIA, through exploitation of software transferred to the Soviet Union, created a damaging attack on Soviet pipeline systems. The software that was used to run the pumps, turbines, and valves of the pipeline was programmed to malfunction after a specific time interval. The malfunction caused the control system to reset the pump speeds and valve settings to produce pressures beyond the failure ratings of the pipeline joints and welds. The result was the largest non-nuclear explosion and fire ever seen from space. There were no physical casualties, but the goal of economic damage was met. This story is an excellent example of the type of attack that can be accomplished by a nation state.

In January 2003, when the SQL Slammer worm began attacking computer networks around the world, users of the business network at Ohio's Davis-Besse nuclear power plant began to notice a network slowdown. Investigation revealed the worm had spread from the plant's business network to its operations network, causing enough congestion to crash the computerized panel used to monitor the plant's most crucial safety indicators. Minutes later, the Plant Process Computer, another monitoring system, crashed as well. The plant's firewall had initially blocked Slammer, but the worm still managed to reach the plant through a high-speed connection from an unsecured contractor's network. Had the plant's operations network been properly protected from either the contractor's network or the plant's own business network—or had the plant operators installed Microsoft's patch to prevent the Slammer infection (released six months earlier)—the infiltration would not have happened. Fortunately, the incident did not result in disaster because the plant was off-line at the time, for regular maintenance, and the crashed monitors were being backed-up by analog counterparts..

These two incidents exemplify the potential consequences of inadequate cyber security processes. We should regard them as warnings.

Sandia's Contributions to Critical Infrastructure Control System Protection

SCADA Security and Standards

During the Clinton administration, Sandia was heavily involved in supporting the President's Commission on Critical Infrastructure Protection. That activity, along with our experience in providing secure information systems for nuclear weapon command and control systems, provided impetus for our initial work in SCADA security. We began our work with laboratory directed research and development (LDRD) funds, and we initiated development of a laboratory SCADA test bed in 1998. At that time it was difficult to convince others of the implications of SCADA vulnerabilities, so we also engaged the standards community. Standards are necessary for improving the security of distributed, networked systems. Because many SCADA equipment manufacturers are foreign owned, the only way to provide trusted systems is through the application of standards. Sandia was designated by the DOE to be the U.S. representative to the International Electromechanical Committee standards working group, TC57. We are expanding our efforts, in collaboration with other national laboratories, by engaging other standards groups like AGA 12–1 ("Cryptographic Protection of SCADA Communications"), API 1164 ("API Security Guidelines for the Petroleum Industry"), and ISA SP99 ("Manufacturing and Control System Security"), as well as various IEEE working groups.

Sandia maintains strong research and development programs in cryptography, network security, secure network architecture design, wireless network security, threat assessment, and intelligent agent-based security approaches. This work is coordinated by our Center for SCADA Security, which was established in 2000.

Red Team and Assessments

Sandia also performs vulnerability assessments of critical infrastructure systems from both cyber and physical security perspectives. We have completed vulnerability assessments of a number of dams in the western United States. We have also assessed the vulnerability of networks used by a number of banks and by the Strategic

Petroleum Reserve. We have worked with the electricity and oil and gas sectors to improve the robustness of their SCADA systems. As a result of these experiences—as well as our own strategic planning, our LDRD investments, and the foresight of sponsors to invest resources toward critical infrastructure protection—Sandia was in a position to immediately address some of the urgent needs following the events of 9/11.

For example, we quickly developed a self-assessment methodology called RAM–W for water treatment facilities; this effort was sponsored by both the Environmental Protection Agency and the American Water Works Association Research Foundation. We also developed training classes on assessing SCADA systems for use in training our own staff. We now provide this training to industry, and we promulgate best practices to industry for securing SCADA systems. These and other contributions to critical infrastructure protection are possible because of strategic planning conducted years ago that led to early investment in the capabilities needed to respond. We also continue to invest LDRD funds in areas of urgent need. Examples include the integration of cyber and physical security technology, cryptographic solutions for SCADA system communications, modeling and simulation of infrastructure elements, secure control of micro-grids, SCADA forensics, and application of new network security technologies to SCADA systems.

Partnering Activities

In 2004, the DOE and the National Energy Technology Laboratory funded the National SCADA Test Bed (NSTB), which is an activity of the Center for SCADA Security at Sandia. Sandia and Idaho National laboratories were designated as co-leads of this effort. Other partners include Argonne National Laboratory, Pacific Northwest National Laboratory, and the National Institute of Standards and Technology. The goals of the NSTB are to raise awareness of, and demonstrate the need for, improved security. The approach is to demonstrate credible threats against critical infrastructures and conduct vulnerability assessments of SCADA systems. We also develop, in collaboration with industry, risk mitigation strategies for current SCADA systems. We are developing new architectures for future secure infrastructures, and we are supporting the development of national guidelines and standards for secure SCADA design and implementation.

Internal Sandia Programs

A number of Sandia facilities support the SCADA security effort, including the Distributed Energy Technology Laboratory, which provides a platform to test the control of operational generation and load systems. We also have a Network Visualization Laboratory that provides both visualization and network modeling capabilities, a Cryptographic Research Facility that supports research and development of cryptographic methods for SCADA networks, an Attack Resource Center that provides tools to attack and analyze SCADA vulnerabilities, and an Advanced Information Systems Laboratory that supports research and development of intelligent agent technologies that may provide self-healing infrastructures in the future.

Sandia also sponsors a nationally recognized College Cyber Defender program that trains university students to protect electronic information and defend computer systems and networks from cyber attacks. The program encourages a pipeline of qualified candidates in the fields of cyber security and protection to address Homeland Security and national security needs.

Research

The Department of Homeland Security has funded the Institute for Information Infrastructure Protection (I3P) to conduct research in SCADA security in order to improve the robustness of the nation's interdependent critical infrastructures. Sandia is the team lead for this project, which includes faculty and staff from ten institutions individually recognized for their expertise in cyber security and critical infrastructure research: Sandia, University of Virginia, New York University, University of Tulsa, Pacific Northwest National Laboratory, Massachusetts Institute of Technology's Lincoln Laboratory, SRI International, MITRE, University of Illinois at Urbana-Champaign, and Dartmouth College. The institute is presently researching the following six high-priority tasks:

Task 1: Assess dependence of critical infrastructures on SCADA and its security.

Task 2: Account for the type and magnitude of SCADA interdependencies.

Task 3: Develop metrics for the assessment and management of SCADA security.

Task 4: Develop inherently secure SCADA systems requirements.

Task 5: Develop cross-domain solutions for information sharing.

Task 6: Transfer technology of these solutions into industry.

The institute represents the type of collaboration needed among private stakeholders, academia, government agencies, and national laboratories to solve the complex problem of SCADA security.

Suggestions for Addressing Critical Infrastructure Control System Problems

Private industry owns about eighty-five percent of U.S. critical infrastructure assets. Industry, therefore, has a key role in implementing protection strategies. Currently, the business case (i.e., return on investment) for industry to invest in increasing the security of their information systems has not been convincingly made. Part of the reason is that no one has been able to clearly define a specific threat. In the past, industry has demonstrated its willingness to invest in protection when faced with a specific threat. The best example of this is the hard work and dedicated effort that industry provided to counter the Y2K threat.

Although we know that many threats exist, specific details are elusive. It may be that we will need to take a consequence-based approach—rather than a threat-based approach—to provide the rationale for the business case. This approach would involve identification of specific portions of information systems affected by specific attacks. It would require vulnerability assessments, analyzing the consequences of disruptions in economic terms, and defining and implementing optimized protection strategies based on risk assessments. The national laboratories use sophisticated means to develop simplified assessment and risk survey processes, like the RAM–W work at Sandia. Risk assessment methodologies can quickly and more broadly identify the current security conditions and help decision-makers plan the most cost effective steps to improve a particular infrastructure's security posture. Increased emphasis should be placed on public-private partnerships in order to make this process efficient.

When considering solutions, the difference between levels of threats needs to be considered. The current emphasis by industry is to try to eliminate inherent vulnerabilities that are present in all networked computer systems. Hackers and hacker coalitions view these vulnerabilities as low-hanging fruit. They exploit them to steal information and identities and/or to deny or disable processes. There is recent evidence that organized crime is also exploiting these vulnerabilities for extortion purposes. Academia and the industrial information security groups are working to provide technology solutions to counter the lower level threat. Until those solutions arrive, all critical infrastructure providers should apply best practices for defense against inherent system vulnerabilities. These practices should include development of security policy as well as technology solutions to provide a sustainable security environment.

At the same time, terrorists and nation states are developing attack methods that are much more sophisticated, often covert. We need new efforts to identify, characterize, and counter these threats. Perhaps this is the proper role for government agencies with technical support from the national laboratories. In that case, the government agencies and national laboratories that are working on high-end defensive solutions will need to establish a plan for technology transfer to industry, because the methods used by today's sophisticated adversary will at some point be available to the lower level threat community.

It is clear that successful defense of the nation's infrastructure will require increased interagency cooperation. For example, the Department of Defense (DoD) has a vital interest in the reliable and secure operation of the nation's critical infrastructures because the U.S. military depends on both domestic and international infrastructures to conduct its missions. Thus the DoD has a keen interest in protecting the SCADA systems that monitor infrastructures, and cooperation with other U.S. agencies will be vital to its mission success.

The Department of Homeland Security (DHS) is already working with the DOE on cooperative interagency projects like the National SCADA Test Bed and the DHS's SCADA security programs. These two agencies should continue their cooperative efforts to ensure that work is coordinated effectively, all threats are considered, the best technology is used, and duplication of effort is avoided. The collaborations and partnerships called for in Homeland Security Presidential Directive 7 (Critical Infrastructure Identification, Prioritization, and Protection), along with the roles and responsibilities described there, are key to accomplishing these goals.

Recommendations

- Reaffirm the concept of public-private partnerships and encourage participants to share information on threats, vulnerabilities, consequences of outages, training, and technology. Extend these partnerships to assist industry in making the business case for investments in security upgrades.

• Increase funding for improvements in cyber security technology, for example: tools for high speed intrusion detection systems, software assurance, attack attribution and trace-back, security modeling of existing and proposed SCADA systems, network visualization for mapping cyber disruptions, triage of threat scenarios across many vectors, and methods for assuring the reliable performance of COTS products.
• Establish and fully fund additional work that provides defense against sophisticated threats.
• Continue Congressional support of the initiatives and directives described in the National Strategy for the Physical Protections of Critical Infrastructures and Key Assets, the National Strategy to Secure Cyberspace, Homeland Security Presidential Directive 7, the Interim National Infrastructure Protection Plan, and associated Sector Specific Plans.

Thank you, Mr. Chairman. I would be pleased to respond to any questions you may have.

ATTACHMENTS

SUPPLEMENTAL STATEMENT OF DR. SAMUEL GLENN VARNADO

SANDIA NATIONAL LABORATORIES

Summary of Major Points

• The nation's infrastructure is highly vulnerable to cyber threats. Supervisory Control and Data Acquisition (SCADA) systems are prime targets for hackers, terrorists, and nation states.
• U.S. computer networks are under daily attack. Adversaries are becoming more sophisticated. We are seeing structured, well-resourced attacks that are designed to steal information or disrupt and/or deny processes.
• Information technology vendors release four new vulnerability announcements each day. At the same time, new attack methods are proliferating. For example, Super Slammer, a fast worm, infected 60% of the Department of Defense's (DoD's) NIPRNET (Unclassified but Sensitive Internet Protocol Router Network) machines in eight minutes.
• Most of the current emphasis in the cyber security community is on responding to hacker incidents. This effort is necessary and useful; however, the work has a short-term focus. We must mature our thinking in the area of enterprise-wide network defense strategies. In addition, more complicated threats such as terrorism and nation state actors must be addressed.
• We have no alternative to the use of Commercial Off the Shelf (COTS) products in all our information systems. Most of these hardware and software products are manufactured in countries whose interests do not always align with those of the United States.
• We must understand that we will be attacked. What are the implications of that understanding, and what strategies do we have in place to operate through the attacks in order to implement recovery and response activities?
• We need to expand our investment in cyber security technology development in order to address the new threat and vulnerability environments.
• We must encourage more public-private partnerships to share threat, consequence, and vulnerability data and to implement cost effective security solutions.
• We must help industries develop a business case for their investment in SCADA security.
• Sandia National Laboratories has been working to improve the security of SCADA systems for over ten years. We have invested laboratory directed research and development (LDRD) and other appropriate sponsor-provided funds into technologies that have direct application to homeland security and infrastructure protection.

Mr. LUNGREN. The Chair would now recognize Dr. K.P. Ananth, Associate Laboratory Director for National Homeland Security at the Idaho National Laboratory, to testify.

STATEMENT OF K.P. ANANTH, ASSOCIATE LABORATORY DIRECTOR, NATIONAL AND HOMELAND SECURITY, IDAHO NATIONAL LABORATORY

Mr. ANANTH. Thank you, Chairman Lungren and distinguished members of the homeland security subcommittee. I am K.P. Ananth, Associate Lab Director for National and Homeland Security at the Idaho National Laboratory, a DOE national lab. It is a pleasure for me to appear before you to represent the work carried out at INL in support of our national efforts to protect critical infrastructure. In this testimony I will give you a short summary of our unique capabilities related to SCADA, critical infrastructure protection, and cybersecurity, the work we do and the challenges we face.

For the last half century, INL has played a key role in the energy security and national security of the U.S. through its pioneering work in nuclear reactors, nuclear power and nuclear ship propulsion, and, as a result, developed a significant infrastructure with one-of-a-kind test beds and facilities on a secure 890-square-mile complex in Idaho. The written testimony provides details on many of the facilities, but I will focus here on those assets directly related to improving cybersecurity and a critical infrastructure protection mission.

Process control systems in SCADA at the INL include a 61-mile, 138-kilovolt transmission line with seven substations and a power distribution control center, a pilot chemical plant, and significant cybersecurity capabilities. We have 10 SCADA test beds with plug-and-play capabilities that a system might need for evaluation. These test beds are secure to protect vendor systems and information and have connectivity to the test range.

Additionally, we work with the global commercial vendors such as ABB, AREVA, GE, Siemens and others, and we enable our work through these vendor systems to look at the system vulnerability and to improve cybersecurity.

Additionally, INL's low radio frequency background, combined with our NTIA status and access to major telecom vendors, enables INL to address risks and improve robustness of communication links. This portfolio of unique test beds complemented with our experienced staff and our collaborators in the national laboratories, academia and industry serve as a national resource for critical infrastructure protection.

Now I will touch upon the key programs we have and results. The DHS program known as US–CERT Control Systems Security Center is aimed at improving control systems security across all critical infrastructure sectors. Key accomplishments include design of a cybersecurity framework and self-assessment tool for industry that is being validated by industry and NIST. This will be piloted in fiscal year 2006.

We support US–CERT in handling control systems-specific incidents and events, preparing bulletins and support for reported events. We have expanded the cyber test bed with three fully functioning systems and tested control systems of vendors showing vulnerabilities and shared them with industry. We have provided training and tabletop demonstrations at 9 U.S. locations to 460 end users.

The DOE program known as the SCADA Test Bed performs testing and analysis focused on the energy sector. We have identified key vulnerabilities in four major control systems used in the electric sector and worked with vendors to develop fixes. We have shared findings with over 200 representatives of 100 major industry owner user groups through invited participation. We provided SCADA security NERC-certified training and other courses to over 350 participants. Through these programs we have helped industry develop and deploy more secure digital control SCADA systems and evaluated technology from providers representing 80 percent of the control systems market for the electric grid.

Now I will move on quickly to the challenges. Increased connectivity. As my colleague mentioned here, control systems today are susceptible to security threats due to open industry protocols and access to control systems information via public networks, legacy systems. Many of the older control systems with long life cycles did not consider cybersecurity; hence, they are vulnerable.

Deregulation. Utility deregulation has increased the number of entities involved in the power life cycle, from generation to transmission, distribution, marketing and billing. Consequently there is increased connectivity and increased potential for cyberattacks via corporate networks.

Offshore reliance. Again, cost pressures and technology support constraints have driven companies to go abroad, again causing security vulnerabilities.

And the need for information sharing is also critical.

Although these challenges are numerous, they are surmountable, and we have got some recommendations that are in the written testimony that you will see.

Mr. Chairman and distinguished members of the group, we invite you to visit Idaho, see the test bed and the work we do in supporting the Nation's infrastructure problems. Thank you.

Mr. LUNGREN. Thank you very much, Doctor.

[The statement of Mr. Ananth follows:]

PREPARED STATEMENT OF DR. K.P. ANANTH

Chairman Lungren and distinguished members of the Homeland Security Subcommittee:

I am Dr. K. P. Ananth, Associate Laboratory Director for National and Homeland Security at the Idaho National Laboratory (INL), a DOE national laboratory. It is a privilege and honor for me to appear before you to represent the work being carried out at INL in support of our national efforts, undertaken in both the federal and private sectors, to protect U.S. critical infrastructure. In this testimony, I will give you a brief background on INL and its mission, and a summary of our unique capabilities as they relate to Supervisory Control and Data Acquisition (SCADA), Critical Infrastructure Protection (CIP) and Cyber Security. I will also discuss key federal and commercial programs carried out at the Laboratory to support industry and end users, and identify the challenges we face along with some recommendations.

INL and its Mission

The Idaho National Laboratory had its origin as the National Reactor Testing Station in 1949 in Idaho Falls with a mission to design, engineer, develop a prototype, and test an electricity producing nuclear reactor. Within two (2) years, in December 1951, INL successfully demonstrated the first electric power reactor and, soon thereafter, developed the first prototype nuclear reactor for the nuclear submarine Nautilus. For more than 50 years, the laboratory has been a critical asset within the National Laboratory system as an engineering, prototyping and testing resource,

with 52 reactors built and operated on the 890 square mile reservation in southeastern Idaho. Beginning in the 1950s, the Laboratory began to support major Department of Defense programs, including training of thousands of Navy nuclear operators; earlier the Laboratory was involved in the development and testing of naval guns and ordnance. In 1985, the Laboratory was selected to produce armor for the Army's Abrams tank using depleted uranium, and earlier this year we successfully completed our twentieth anniversary on the program.

To support these varied missions, INL has developed a significant infrastructure on the Idaho desert. INL carries the distinction of a vast, remote, and secure heavily-invested site complex with "one-of-a-kind" test beds and facilities for nuclear research and development (R&D), explosives detection and testing, unmanned aerial and ground vehicles payload testing, physical security, cyber security and critical infrastructure protection. Mindful of the rich assets at INL, the Department of Energy issued a Request for Proposal (RFP) in 2004 to manage and operate INL with the mission of ensuring the nation's energy security with safe, competitive, and sustainable energy systems and providing unique national and homeland security capabilities. Two areas were specifically called out within national and homeland security for the Laboratory: nuclear nonproliferation and critical infrastructure protection. On February 1, 2005, the new contract to operate the Laboratory was implemented, making the critical infrastructure protection mission of the Idaho National Laboratory unique within the National Laboratory system. We are hard at work fulfilling this mandate.

Today I will focus on how we are leveraging our efforts with DHS and DOE in the area of improving control systems security across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk.

INL's Unique Assets

With more than five decades of experience in establishing, developing and maintaining critical infrastructure systems, INL has created several recognized and integrated capabilities to provide real solutions to our customers in critical infrastructure protection and cyber security. INL has focused in three major areas—process control systems, cyber security, and wireless technology.

Process Control Systems (PCS) and SCADA—Our location and operational infrastructure provides the ultimate proving ground for analysis and assessment of real-world critical infrastructure components. INL has become the logical home for significant portions of the National SCADA Test Bed and has become the focal point for research and testing of control systems and cyber security with a direct benefit of increasing the security of these systems. INL operates a power distribution control center, a pilot chemical plant, and 61 miles of 138 kV transmission line with seven substations and a dedicated control room on our 890 square mile site. It is the combination of this infrastructure, a program with current access to commercial control systems from principal global vendors (e.g., ABB, AREVA, GE, METSCO, Micro Motion, [Emerson], Rockwell Automation, Siemens), and our research expertise and partners that enables us to conduct offline and full-scale testing in a real life environment. This unique capability is helping to research and develop solutions that will strengthen our nation's industrial control systems and physical components of our infrastructures from attacks by viruses, hackers, and terrorists.

Cyber Security—the INL Cyber Security Group's intimate familiarity with various hacker methodologies enables us to generate exploits and assessment tools for use in testing the security of Critical Infrastructure control system environments. Focused on multi-tier attack vectors and full spectrum threat actors, the team provides a credible representation of cyber threats and then conducts cutting edge research into advanced mitigation strategies and solutions. Coupled with our academic and industry partners in this area, we are striving to effectively address current challenges while advancing the state-of-the-art in detecting hacker signatures. We have invested resources to explore the cyber security vulnerabilities of Portable Electronic Devices (PEDs) technology. INL is pursuing commercial and government partnerships to address vulnerabilities in PEDs technology because these devices are becoming more prolific and have crept into new control systems.

Wireless Technology—INL's Wireless Test Bed and telecommunications infrastructure provides access to advanced, next generation communication technology and current communication systems to analyze vulnerabilities, analyze new protocols and operational performance, and develop risk mitigating solutions. INL's location providing a low RF background, our National Telecommunications and Administration (NTIA) experimental radio station status, full-scale isolated communications networks, and ability to connect to functional systems has attracted industry (e.g., Bechtel Telecommunications, Nokia, AT&T Wireless) and government customers. Bechtel Telecom, through a Cooperative Research and Development Agree-

ment (CRADA), has made a significant investment at the Laboratory in this area. These attributes afford us the unique opportunity to holistically analyze both performance and risk of entire systems, develop wireless security solutions for our nation's complex, interconnected infrastructures, and improve robustness of communication links for emergency responders.

The importance of these core assets can not be overlooked, representing a national resource that provides access to control system hardware and applications, functioning transmission and distribution assets, wireless local and metro area networks, advanced radio, microwave, fiber optic and satellite communications, mesh networks and personal electronic devices (PEDs). Additional assets include unmanned aerial vehicles (UAVs), explosives detection, testing and blast mitigation systems. Perhaps more importantly, our current network of industry participants and top shelf researchers across the nation enable INL to address the most challenging issues in CIP.

These are the elements—housed in our comprehensive test range, designed to be full-scale in nature, representative of real world infrastructures and capable of being isolated—that uniquely position the federal government, national laboratories, and industry to be successful in identifying and managing risk to our nation's critical infrastructure. To the best of our knowledge, there is no similar facility in the world. And, the cache of over 100 experienced scientists, engineers, and technicians working in INL's SCADA/Cyber Security groups are aware of the great responsibility that comes with managing these resources and the significance of our mission to assist in securing the control systems of our nation's critical infrastructure. With this knowledge, we have focused on developing extensive collaborations on our programs and continually strive to bring the best-in-class institutions to help in developing solutions to this complex challenge. Our collaborators in this area include other national laboratories, National Institute of Standards and Technology (NIST), American Society of Mechanical Engineers (ASME), Instrumentation Systems and Automation Society (ISA), Carnegie Mellon University (CMU), Dartmouth University (DU), University of Idaho (UoI), British Columbia Institute of Technology (BCIT), and others such as North American Electric Reliability Council (NERC), Electric Power Research Institute (EPRI), Chemical Industry Data Exchange (CIDX), Decision Analytics Corporation (DAC), KEMA Consulting and Bearing Point.

Key Programs Conducted at INL and Results Achieved

Our two primary programs in Cyber Security and Critical Infrastructure Protection are with the Department of Homeland Security National Cyber Security Division and Department of Energy Office of Electricity Delivery and Energy Reliability. INL is supporting both programs with a team of talented people from other national labs, academia and industry based on their best-in-class core competencies and the needs of the program.

The DHS program is known as the "US-CERT Control Systems Security Center (CSSC) Program." This program is aimed at improving control systems security across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk. One of the key tasks of this program was the design of a cyber security protection framework consisting of a comprehensive set of requirements, graded recommendations/solutions, and automated self-assessment tools for all sectors to use to enhance the security of their control systems (e.g., SCADA, DCS) against cyber attack. The draft framework was issued in July 2005 and reviewed with 20 industry control systems and cyber experts; and a second review occurred in August with several key industry security managers. Comments to date have been:

". . . .framework provides a centralized, organized approach to Control System security. . ."

". . . .provides actionable recommendations. . ."

". . . .provides a benchmark and metrics for cyber security protection. . .

". . . .will help consolidate the efforts by the Standard bodies
. . ."

". . .provides for cross platform standardization across vendor products
. . ."

". . . .impressed with the automated self-assessment tools that will measure improvement
over time
. . ."

We have plans to work with NIST and ISA over the next three months to assist us in implementing the cyber security framework for self assessment. We will also work with facilities in several key sectors in FY-06 to pilot and validate the framework. A key component of the self assessment will be a risk reduction tool that

helps companies prioritize vulnerabilities that are found when assessing requirements and potential consequences.

Additionally, the program also developed a quick response cell to support US CERT in handling control system specific incidents/events. We have assisted in preparing cyber security bulletins and providing Tier II support for reported events to the US-CERT.

Over the last two years, we have collaborated with DHS and DOE to significantly increase the capabilities of our extensive cyber test bed. This capability includes ten (10) SCADA test beds and three (3) fully functioning systems that are ready and are currently testing vendor systems and specific tools to reduce cyber vulnerabilities. On the CSSC program, we are currently testing three (3) vendor control systems and have already identified significant vulnerabilities on the first two systems. The vendors are evaluating the results and our recommendations.

The purpose of this program is to reduce risk to key infrastructure from cyber attack by enhancing the security of control systems. To that end, we have developed a risk assessment methodology for control systems to measure vulnerability reduction and we have developed decision analysis tools. We have started validating these tools by analyzing test results and attack scenarios.

Our industry outreach efforts provide unique training by demonstrating how an attack may propagate through the business system to critical control systems with an emphasis on how to mitigate the effects of such an attack. These awareness demonstrations and training activities are ongoing with positive feedback from industry and government participants. The tabletop demonstrations have included live demonstrations of attacks/effects on small scale representative control systems for chemical and electric system processes and demonstrations of attack mitigation strategies. We have held these demonstrations at nine (9) venues across the U.S. with over 460 end users participating from a wide variety of industries to include control systems/cyber security organizations and federal, state and local government agencies.

Through this program, we are also providing SCADA and process control security training for the protection of dams and hydroelectric facilities to system users in the Department of Interior's Bureau of Reclamation.

The DOE program, known as the "National SCADA Test Bed (NSTB) performs testing and analysis of SCADA systems representative of those used throughout the energy sector to identify, validate and reduce cyber vulnerabilities. The second objective is to identify best practices for design and deployment of secure control systems and to support institutionalization of those best practices in government and industry standards. The NSTB is a joint effort between Sandia National Laboratory and Idaho National Laboratory. The NSTB effort is managed by the INL and includes, Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and the SCADA vendor community (ABB Network Management, AREVA T&D Automation, GE Energy Management Systems, Siemens Power Transmission and Distribution), as well as computer system vendors such as IBM, HP, and Sun Systems. Key accomplishments on this program include:

- The NSTB has identified SCADA vulnerabilities in the four systems INL has tested, worked with the SCADA vendors to define/develop fixes where needed, and verified the fixes through follow-on testing. SCADA vendors have improved new releases and developed patches to mitigate significant security weakness. These risk reducing actions will directly benefit many of the nation's critical infrastructure organizations.
- We have shared the findings from these SCADA system vulnerability assessments, in various levels of detail, with over 230 representatives from 100 major industry owner/user organizations through invited presentations at SCADA vendor users' group meetings.
- We have issued detailed test reports of the SCADA assessments to the respective vendors. One of the vendors is sharing their assessment report, under tight non-disclosure agreements, with all interested users.
- Through the participation of SCADA vendors who have been willing to loan their systems to INL on the NSTB program for an extended time, we have established an extensive, representative environment for searching out typical security vulnerabilities and for testing solutions.

We developed and presented a NERC-certified training course on SCADA security. Based on feedback from the initial presentation of various courses (NERC and others) to over 350 participants, we are expanding the content and are now responding to requests for additional presentations.

Commercial Programs—INL has helped industry develop and deploy more secure digital control/SCADA systems, through vulnerability discovery, validation and mitigation, standards development and secure software technology.

Specifically, the INL managed National SCADA Test Bed Program (NSTB) has worked with global control system software vendors to promote more secure , innovative installation and implementation of their products, where such efforts are consistent with recognized industry guidelines and best practices. The program has discovered existing weaknesses in deployed systems as well as design weaknesses in future control systems. The program has evaluated technology from providers representing 80% of the electrical grid control system market, working closely with engineering teams of four (4) global providers.

We have worked with control system owners and operators across multiple sectors to evaluate and enhance security of existing technology deployments. These companies took advantage of the unique knowledge-base and trusted relationships at the Lab as an important element to their overall approach to critical systems risk management. Companies have also turned to us when things go wrong with the systems to assist in evaluating particular events to determine if directed or non-directed attacks might have occurred.

With most of the critical infrastructure residing in the private sector we felt it was appropriate to submit just a few comments from the asset owners themselves. These perspectives come from private sector organizations from the trenches to the executive offices best demonstrating the value of government sponsored CIP initiatives at INL:

1. David Norton, Transmission IT Security program manager for Entergy—New Orleans (the second largest generator of electricity in the U.S. delivering electricity to 2.7 million customers), wrote "We are in dire need of INL, its mission, and its uniquely qualified staff. I know of no other entity in North America doing anything like what they are doing in the field of SCADA control system security, and certainly not to the level of excellence that I and my peers in the industry have witnessed."
2. Cheryl Santor, Information Security Manager, Metropolitan Water in California (one of the largest water systems servicing 5,200 square miles in Los Angeles, Orange, San Diego, Riverside, San Bernardino and Ventura Counties with 18 million customers), wrote "The INL provides a knowledge base from which all organizations using SCADA and Process Controls can benefit. . . .in order to secure their critical resources."
3. Phil Harris, CEO of PJM (Ensuring the reliability of the largest centrally dispatched Control area in North America by coordinating the movement of electricity in all parts of Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia, and the District of Columbia), wrote "PJM feels it is important that the Electric Sector, as a Critical Infrastructure support INL and the work they do. There is no substitute or other entity that is providing such quality service of such national importance."
4. Another utility security executive from American Electric Power recently testified to the value provided by INL through the DHS and DOE program: "The electricity industry is interested in continuing to work closely with DOE on the work being done at the Idaho National Laboratory. We believe it holds great promise as one of the best and most efficient means of stimulating research and developing technical solutions to the present shortfalls in cyber security." [Hearing Before the United States House of Representatives Science Committee, September 15, 2005].

Key Challenges in CIP and Cyber Security

As a result of operating and testing infrastructure systems, working with control system vendors and end users, INL is keenly aware of the key challenges in protecting critical control systems and the potential solutions to these complex challenges to ensure the security of our nation's critical infrastructure.

• ***Increased Connectivity***—The use of open systems and more common technology combined with greater system access and available system knowledge has changed the risk profile of SCADA systems. These systems evolved in a less connected world relying on proprietary technologies which provided a sense of "security through obscurity" in the past. The control systems of today are more susceptible to security threats than before with SCADA vendors increasingly moving toward open industry standard protocols and platforms, system owners and operators providing greater access to market and accounting systems, regulatory requirements to share information and make systems available to all market participants and the greater use of public networks and wireless communications.

• ***Interdependencies***—A further challenge arises from the reliance on telecommunication as an integral part of the overall control system. If SCADA and Energy Management Systems (EMS) are the brain stem and receptors of a control system, then 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. [The following provides a useful reference: Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, February 2005]

• ***Complexity***—A particular challenge is the complex and interconnected nature of critical control systems which can be found across many of the critical infrastructure sectors from directing advanced manufacturing systems to controlling the North American electric grid. If we focus on energy production and delivery, we find Process Control Systems (PCS) and specifically SCADA systems are used extensively throughout the electric, oil, and gas sectors to monitor and control processes that generate, transmit, transport and distribute energy.

• ***Legacy Systems***—A significant portion of the control system technology in place today in many installations is old. These legacy systems were designed to operate over long lifecycles and were not designed with cyber security in mind. Hence, they are vulnerable to cyber attack and, in many cases, difficult to protect. In order to significantly lower the risk, we need to understand legacy system vulnerabilities and develop cost effective means to mitigate them without relying on new system deployments.

• ***Deregulation***—Market forces, to include deregulation in the electric utility industry have increased the number of entities involved in the power life cycle from generation through transmission, distribution, metering, and billing; thus increasing reliance on and accuracy of information from third parties. Correspondingly, this has come with increased connectivity with outside vendors, customers, and business partners which have eroded the sanctity of the network perimeter. More connections through the perimeter inherently introduce more threats into the corporate networks.

• ***System Accessibility***—The convergence of power company networks and the demand for remote access to these systems has rendered many SCADA systems accessible through non-SCADA networks. Specifically, connections between the grid and corporate networks for reporting purposes and outage management interfaces have the potential to expose the grid network to the threats experienced by the more common business network. [The following provides a useful reference: U.S.-Canada Power System Outage Task Force, August 14th Blackout: Causes and Recommendations, April 2004].

• ***Offshore Reliance***—Cost pressures and technology support constraints have increased reliance on offshore development and system maintenance, thereby increasing the risk of intentional or unintentional security vulnerabilities. This risk is amplified as a result of ineffective/non-enforceable cyber laws in the respective offshore countries.

• ***Information Sharing***—Finally, competitive pressure, legal liability risk and the lack of information protection mechanisms pose a significant barrier to information sharing between critical infrastructure stakeholders. This has significantly impeded the discovery and understanding of control system vulnerabilities, as well as the reporting of real-world incidents. [The following provides a useful reference: CRS Report for Congress – Government Activities to Protect the Electric Grid, October 2004]. On the other hand, the knowledge revolution that has accompanied the Internet makes it easy to locate specific information regarding SCADA and automation systems. For example, "over 90% of major SCADA and Automation vendors have all of their manuals and specifications available online to the general public" (SCADA Security Strategy, PlantData). Easy access of such information to potential threat actors is a concern.

Recommendations

These challenges, although numerous and complex, are surmountable. There is an urgent need to accelerate the research, development, testing, and application of advanced control systems to enhance cyber security across the energy and other sectors. This need transcends individual companies, energy subsectors, and even the private sector. Toward this end, the Department of Homeland Security and the Department of Energy are supporting programs to facilitate and support risk reducing solutions. We, at INL, are focused on providing solutions to this key national need and have some recommendations for meeting the challenge.

SCADA/Cyber/Telecom Interconnect—We, as a nation, should develop an interdependent and inclusive view of control systems to include not only the SCADA systems but the cyber and Telecommunications functions that support them to ensure secure electrical power and industrial processes. SCADA, Cyber Security, and Telecommunications are areas where we must integrate research and testing efforts to understand how vulnerabilities impact the entire system. We at INL are already engaged with the telecommunication firms on interoperability and bandwidth issues, and we see the SCADA/Cyber/Telecom interconnectivity as the next area of pursuit.

The 21st Century could be characterized as a globally interconnected "flat world" (courtesy of Tom Friedman), which means hierarchical systems have to yield to horizontal and partnership-based enterprises. To that end, critical infrastructure protection, cyber security, and telecommunications particularly call to attention the interdependence between providers and markets so industries have a responsibility to work across sectors, and the same holds for the federal government. Furthermore, in the event of a manmade or natural disaster as in Katrina, active coordination across sectors is vital for timely response and expeditious recovery.

Minimum Standards—The electric sector, being at the hub of all, is active in securing its cyber and physical resources. Interim cyber security standards are in place in the electric sector, and they are moving through the approval process for a permanent, more expansive CIP standard. The final product should strengthen cyber security across the electric sector and lay the groundwork for greater collaboration between industry and government. Similar efforts are underway through CIDX and much work remains to be done in all sectors of our infrastructure.

Develop Risk Assessment Tools—The federal government should continue to invest in the development of tools and provide required information to assist control systems security professionals to identify and address risk. Education and awareness efforts should be focused on developing an accurate understanding of risk to control systems. The NSTB Program and the CSSC program are both actively addressing this need and risk mitigation steps are beginning to be implemented at the user level.

Fixing Legacy Systems—Some type of incentive, either at the vendor level or user level, will go a long way to implement cyber security in legacy process control systems. Coupled with independent third party testing of the control system, through programs such as NSTB and CSSC, legacy systems could be upgraded with protective measures.

Information Protection—The electric infrastructure is one of the most critical infrastructures servicing the nation and maintaining our way of life. Certain technical, architectural and operational aspects and details must be kept secure so they will not be inadvertently disclosed to those who would try to disrupt or destroy our social, political or economic fabric. Yet there is a need to share the security aspects of the information with government and industry peers for benchmarking purposes while preserving competitive advantages. The same challenge applies to other sectors as well. This is an area where the use of trusted independent third party entities might prove beneficial and acceptable to all parties and merits further discussion.

Concluding Statement

Mr. Chairman and distinguished Members of the Committee, we at Idaho National Laboratory are fully committed to deliver on this important national mission, and along side DHS, DOE, and industry, we will strive to make our Laboratory the Center of Excellence in critical infrastructure protection to help end users. We welcome you to visit the Idaho National Lab to see firsthand the solutions we are providing to make our infrastructure safer. Again, I thank you for the opportunity to share these comments with you.

Mr. LUNGREN. The Chair would now recognize Dr. William Rush, institute physicist at the Gas Technology Institute, to testify.

STATEMENT OF WILLIAM RUSH, INSTITUTE PHYSICIST, GAS TECHNOLOGY INSTITUTE

Mr. RUSH. Good afternoon, Mr. Chairman and members of the committee. I would like to thank you very much for letting me testify on what I think is a really important topic. I am Bill Rush. I hold a Ph.D. in physics, and for the past 27 years I have been with

the Gas Technology Institute, or GTI. I also chair the American Gas Association's Encryption Working Group, which is charged with developing cryptographic protection for SCADA communications.

Today I am going to update you on the nuts and bolts of what it is that we have done to protect against cyberattack and recommend some specific steps for improving SCADA security.

As you know, attacks against SCADA are of concern because SCADA is the remote control, if you will, of a network. It controls the circuit breakers and the valves. It is the actual "reach out and grab things" part of the system. Most systems were designed before security was regarded as a serious concern and as a result are poorly protected against cyberattack. One team of U.S. network experts was into a SCADA system within 15 minutes.

Can cyberattack have real consequences? Absolutely. As Dr. Varnado pointed out, a 3-kiloton explosion, to put that into more usable or more familiar terms, that is about 1,000 times as powerful as the explosion that blew up the Murrah Federal Office Building in Oklahoma City.

SCADA information has been found on captured al-Qa'ida computers. Three weeks after the 9/11 attacks, the American Gas Association chartered the AGA 12 Working Group to develop a standard to protect SCADA communications. The drawing that we have up here indicates basically how it works. What you do is originate a command, such as open the switch inside a secure facility. It then gets sent into a cryptographic module which changes the message, and as you can see across the bottom, it can't be read by anybody without a special number that is called a key. When it shows up on the other end, it is decrypted by the same key and turns back into the message, open the switch.

AGA 12 team is proud of its progress to date, but this is not just a paper standard. This device that I have brought with me, and you can see it afterwards, is an AGA 12-compliant cryptographic module. This unit effectively slams the door in the face of those who would attempt to penetrate the communication networks of SCADA systems. Early versions of this equipment has performed well in the field tests. This unit is priced at about $500. It can be installed right now in most SCADA systems that operate on low-speed links. Nationally labs are in the process of evaluating its security level and its performance. At least two manufacturers will market AGA 12 modules. No other standard groups can provide this protection today.

While many groups contributed to AGA 12's success, none did more so than the Navy's Technical Support Working Group, or TSWG. TSWG funded GTI to work on AGA 12 full time. This allowed us to move far faster than any other all-volunteer groups.

Note that AGA 12 is only one of dozens of groups who are involved in developing standards. There is a significant risk of developing conflicting standards. These volunteer groups lack the resources to coordinate their efforts. The DHS Process Control Security Forum and DOE's Roadmap are important examples of government and private sector coordination in cyber security.

Regrettably, AGA 12 has become a victim of its own success. TSWG only funds prototypes until they succeed. When AGA 12

passed this milestone last May, both funding and progress ceased with a serious loss of momentum. Our early success obscured the fact that critical work remains. DOE is providing some funding to go restart tests and to edit parts of AGA 12 for publication, but there is still critical work, including developing a seal of approval conformance testing to show that a product such as this really meets the standard, sort of a Good Housekeeping seal of approval; next-generation designs to work faster and at half the cost; a major pilot test to validate that the technology really works; and remote key changing so you don't have to send staff out when you make changes; and forensic tools to find and prosecute attackers.

In summary, we make the following recommendations: Fund R&D to develop protection against cyberattacks on the Nation's critical infrastructure. Prevent loss of momentum by avoiding program interruptions. This is very disruptive. Support the coordination effort, such as the Process Control Security Forum and the Roadmap. Complete the remaining AGA 12 work that I have just outlined. Support other selected standards works in addressing the many vulnerabilities that are beyond the scope of AGA 12.

Mr. Chairman and subcommittee members, we applaud your focus on securing our Nation's critical infrastructure, especially the area of SCADA protection. I would be pleased to answer questions afterwards. Thank you.

Mr. LUNGREN. Thank you very much, Dr. Rush.

[The statement of Mr. Rush follows:]

PREPARED STATEMENT OF DR. WILLIAM F. RUSH

INTRODUCTION

Good afternoon Mr. Chairman and members of the Subcommittee. Thank you for the opportunity to address you today on this important topic. My name is Bill Rush and I hold the position of Institute Physicist with the Gas Technology Institute (GTI), where I have worked in the field of natural gas technology research and development for 27 years. GTI is a not-for-profit Research and Development institute headquartered in Des Plaines, Illinois. I also am the Chairman of the American Gas Association's SCADA Encryption Working Group. The American gas industry has charged this group with developing cryptographic protection for gas, water, and electric SCADA communications.

The focus of my testimony today is to update you on the steps the American Gas Association AGA, GTI, and many other organizations have begun to take to protect SCADA communications from cyber attack. At the conclusion of my remarks, I will provide recommendations to the Subcommittee on what actions can be taken to further advance the security of industrial control systems for critical infrastructures.

SCADA SYSTEMS ARE OFTEN VULNERABLE TO CYBER ATTACK

Supervisory Control And Data Acquisition (SCADA) systems are an important component of critical infrastructure. SCADA systems can be thought of as the "remote control" part of most gas, water, electric, and oil pipeline systems. SCADA Remote Terminal Units (RTUs) read the pressures, voltages, temperatures, and flows at critical points throughout the transmission and distribution portions of these critical infrastructure networks and transmit this real-time data back to central control rooms. They also operate valves, circuit breakers, and switches and are thus critical equipment for control of the systems. This remote control of unmanned facilities provides quick response to changing situations, while providing cost-effective operations of a multitude of critical equipment and stations, spread over a large geographic area. Many SCADA RTUs have "maintenance ports" that enable operators to change critical system parameters remotely, open or close valves or breakers, or download new firmware. There are strong similarities among gas, water, electric, sewage, and oil SCADA systems. Process automation and control systems used in other critical infrastructure applications, such as oil refineries and chemical plants, may not have the long-distance aspects of SCADA, but share many other characteristics.

The cost constraints under which SCADA systems operate determine many of their security-related characteristics. Because SCADA systems are expensive to replace, they have long life times—typically between 10 and 20 years. Consequently, many systems now in service have been there for a long time and will remain as legacy systems for some time to come. Consequently, today's SCADA systems are often based on technology which is a decade old. In particular, many of these systems operate at relatively low communication speeds over telephone modems, speeds which most Internet users of today find unacceptably slow.

Because these systems were designed before critical infrastructure security was a major concern, they often have significant vulnerabilities to unauthorized electronic operations, referred to as "cyber attacks". Many of the systems do not have effective password protection for access control or encryption for confidentiality of data and commands. When they use dial-in telephone modems, they often can be hacked from any computer with a phone modem. When the SCADA system uses radio communication, the radio waves can often be detected and altered by a third party with an appropriate, commercially available receiver/transmitter. The question confronting skilled cyber attackers is less "Can we enter the system?" and more "How long will it take us to penetrate it?" The North American Electric Reliability (NERC) is concerned about the ability of an attacker to use the maintenance ports to attack SCADA systems by making unauthorized changes in critical system parameters. Information on American SCADA systems has been found on captured al-Qa'ida computers.

Cyber attacks are not simply minor incidents involving mildly annoying hackers, but can have significant operational, economic, and safety consequences. A single example that underscores this point is the Soviet Union's use of stolen American SCADA software during the 1980's. This code—which had been deliberately modified to cause harm to a SCADA system—led to physical damage to the Soviet SCADA system resulting in an explosion large enough to be photographed from space and estimated at 3 kilotons TNT equivalent. (See "At the Abyss: An Insider's History of the Cold War", Thomas C. Reed, Ballantine Books, New York, 2004.) To put the 3 kiloton number into perspective, the Murrah Federal Office Building bombing in Oklahoma City was estimated at 0.002 kiloton and the Hiroshima nuclear bomb was between 14 and 20 kilotons. The salient point is that it clearly is possible to cause significant physical damage to critical infrastructure if the SCADA code can be modified.

AGA 12 IS A STANDARD TO PROTECT SCADA FROM CYBER ATTACK

Three weeks after the 9/11 attack, AGA chartered a working group to develop a comprehensive standard that would use cryptography to protect SCADA communications from cyber attack. This standard has been designated "AGA 12". When it is completed, it will be a comprehensive approach to SCADA cryptography. The charter instructed the working group to develop a recommended practice for the gas industry and to include water and electric SCADA systems as well. This approach also applies to sewage and oil pipeline SCADA systems. This effort has made such significant progress that we are now field testing commercial prototypes of products that use cryptography to protect SCADA communications.

As a standard, AGA 12 has several significant characteristics. First, it is an open consensus standard that is designed to produce interoperable cryptographic products. "Open" means that anyone can use the standard to build equipment without needing to pay a royalty or licensing fee. Open here also refers to the process by which anyone with an interest in the topic can participate in developing the document. The working group included this requirement to encourage market competition to drive costs down, since no one has a monopoly position. The open-source code for implementing AGA 12 is available for free on the Internet. AGA 12 is a consensus standard because the working group develops consensus among its members and the AGA membership as well that its recommendations are indeed a sound practice. Finally, the standard specifies a minimum level of interoperability among products made by different manufacturers. Thus, users will have a choice of suppliers. The standard also assures that new products will remain compatible with earlier versions. Finally, AGA 12 provides strong protection; it is based on well-established NIST encryption standards and has been examined for its ability to protect against a wide variety of attacks.

AGA 12 is a suite of 4 documents, designated Parts 1 through 4. The four documents address different aspects of SCADA communication protection.

AGA 12, Part 1 (AGA 12–1) summarizes cyber security policies, the background of the cyber security problem, and a procedure for testing cryptographic protection systems. This document educates SCADA operators on the need to do a risk assess-

ment and recommends an approach for those utilities whose risk assessment reveals a need to protect their systems with cryptography.

AGA 12–2 is a detailed technical specification for building interoperable cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and dial-up maintenance ports.

AGA 12–3 will describe how to protect high speed communication SCADA systems.

AGA 12–4 will describe how to build next generation SCADA systems so that their cryptography will be compatible with the legacy systems; this will ease the transition to the newer designs.

Parts 1 and 2 are close to completion. Parts 3 and 4 are in the planning stage.

Figure 1 illustrates both the configuration of a SCADA system and the scope of AGA 12. On the left is the Control Room, which is manned around the clock and where critical operational decisions are made. On the right is the "Remote Terminal Unit" (RTU), which is typically unmanned and controls the sensors and actuators that operate the critical infrastructure. Both the Control Room and the RTU are assumed to be secure. The AGA 12 working group deals only with the issues of security of messages while they are in transit over an insecure network and leaves to others the responsibility for securing the rest of the system.

It is important to recognize that while cryptographic protection of SCADA communications is an important weapon in the arsenal of tools that can protect SCADA, it is only one tool among many that are needed. Cryptography can not provide any protection at all against many kinds of attacks. In particular, it does not protect against jamming or breaking the communication line, against physical attacks, or against many kinds of insider attacks. Nor does it protect local facility control systems1 that are often connected to SCADA systems, and usually offer additional independent vulnerabilities to cyber attack. These issues are being addressed by literally dozens of groups working in the security area. While I am focused only on the AGA 12 effort, I am pleased to report that there are so many security initiatives under way that coordinating their work is a major challenge. I would call your attention to both the Department of Energy's Roadmap to Secure Control Systems in the Energy Sector and the Department of Homeland Security's Process Control Systems Forum as good examples of how the Government is working effectively with the private sector to advance and coordinate the many security efforts that are now under way. I also call your attention to the Instrumentation, Systems and Automation Society's (ISA) ISA SP99 committee, "Manufacturing and Control Systems Security". This is a broad industry wide automation and control systems security standards effort that has published over 150 pages of guidance on how to establish automation systems security programs and available technologies to deal with unacceptable risks. Finally, the National Institute of Standards and Technology (NIST) has produced many standards on which AGA 12 has relied and operates the Process Control Security Forum (NIST PCSRF) which continues to advance putting the cause of cyber security on a firm basis.

AGA 12 SPECIFIES CRYPTOGRAPHY TO PROTECT SCADA COMMUNICATIONS

AGA 12 uses cryptography to protect SCADA communications. Figure 2 illustrates the basic idea of how this works. Data and commands ("Open Switch" in this figure) originate inside of a secure facility, as illustrated in Figure 1. Prior to leaving the secure facility, the data or command is sent to a "SCADA Cryptographic Module" (SCM) which encrypts it. Essentially, this encryption step changes the message so that it can no longer be read by anyone without a special number, called a key. In operation, the encrypted message is sent over the insecure network in an unintelligible form. When it arrives at the designated secure facility, the key is used to decrypt the message, returning it to its original meaning, "Open Switch".

The AGA 12 standard has gone to great length to assure that encrypted messages are very difficult for potential attackers to use to harm a system that uses SCADA. This "link encryption" approach has been used successfully for many years by the financial community to secure its transactions. While this discussion has only considered making the message hard to read, AGA 12 also makes it difficult to alter, forge, or record and replay a message. An important issue associated with AGA 12 is how these secret keys are managed. The keys must be changed periodically to prevent their being guessed or compromised. Different keys are used for employees with different responsibilities and different levels of authority. The authorization to use keys must, for example, be changed if an employee leaves. It is important to be able to do this without the expense of visiting the many distant sites that may be controlled by the SCADA system.

Because of the long life of SCADA systems, the owners and operators of these systems urged the working group to focus first on the challenging problem of protecting legacy systems. Focusing on next-generation SCADA systems first would leave the legacy systems unprotected for many years. Protecting legacy systems, however, required developing cryptographic modules that will support most of the roughly 150 types of existing SCADA systems, each of which has a different "SCADA language" and which operate at different communication speeds and over a wide variety of communication media (such as telephone, radio, and microwave.) The next steps are to develop the same standard protection for high speed and next generation SCADA systems.

AGA 12 HAS MADE RAPID PROGRESS FOR A STANDARD

AGA 12 has made rapid progress, given the constraints that an open group is developing a consensus standard. This is a process that is generally slow for two reasons. First, developing consensus among users, manufacturers, and cryptographic experts on a difficult technical task is a challenging task. Each group has different needs and understanding levels for the standard. Second, most standards development efforts are all volunteer activities. This limits the rate of progress to what can be accomplished in an overload or spare time mode by people with full-time job responsibilities.

Those of us who have participated in the AGA 12 process are proud of the success we have achieved, for this is no longer just a paper standard. AGA 12 Part 1 is in the final stage of balloting prior to being adopted as an industry recommended practice. Two manufacturers are offering or soon will offer cryptographic modules that comply with AGA 12, Part 2. Early versions of this equipment have performed well in field tests at actual gas companies. AGA 12 has entered the field test stage at least 2 years ahead of any other group developing an open standard for cryptographic hardware.

MANY GROUPS HAVE CONTRIBUTED TO THE SUCCESS OF AGA 12

Many groups have contributed to the success of AGA 12. No single group did more to accelerate the work of AGA 12 than the Technical Support Working Group (TSWG), a part of the Combating Terrorism Technology Support Office. TSWG began support of cryptography for SCADA systems with a project at GTI in 1998, well before terrorism was recognized as a threat. While as previously mentioned, most standards groups operate on an all volunteer basis, TSWG funded GTI to provide full-time support by several people to work on AGA 12. This allowed us to debate approaches, build models of the various ideas, test to see what does and what does not work, write our results into the emerging standard, and begin the cycle anew with a debate on the next issue.

In addition to TSWG support, several other government agencies have contributed to the progress of AGA 12. The National Institute of Standards and Technology provided funding to help develop a standard test methodology for evaluating how much cryptography slows communications in network. Sandia National Laboratories evaluated the security level of the first version, work which led to several significant improvements to AGA 12. Pacific Northwest National Laboratory conducted a preliminary test on the impact of AGA 12 on communication speed. Under DOE sponsorship, both of these laboratories continue to do work on the security and performance of the AGA 12-compliant cryptographic modules. These National Laboratory tests are particularly important to the private sector's acceptance of the AGA 12 standard as both secure and functional.

In addition to government support, industry groups have helped. Both AGA and the American Water Works Association Research Foundation (AWWARF) have provided funding and substantial in-kind support for the AGA 12 standard. GTI and the Gas Research Institute have funded the AGA 12 work as well.

Many private companies also supported the AGA 12 project. These include Cisco, OPUS Publishing, SafeNet Mykotronx, TecSec, Schweitzer Electronic Laboratory, Thales e-Security, and Weston Technology. Peoples Energy (Chicago) and Detroit Edison have also been supportive and contributed extensively to the working group's understanding of the needs of SCADA operators.

DESPITE REMAINING WORK, AGA 12 HAS SLOWED SUBSTANTIALLY

Although significant work remains to be done to complete the AGA standard, progress stopped in May of 2005 when TSWG funding ran out. TSWG is an organization which only funds prototype developments until they prove successful, at which time funding is to be provided by other organizations. DOE has supported Sandia and Pacific Northwest National Laboratory to evaluate the security level of the standard and the speed of its encryption, respectively. In October, DOE provided limited funding for GTI to complete some field testing and write up the existing

version of AGA 12–2 as a document that is in a suitable format for ballot. This 5 month hiatus significantly reduced the momentum of the AGA 12 project. Largely as a result of these delays, one of the three manufacturers that originally committed to produce AGA 12 modules has stopped work on this project.

Regrettably, AGA 12 became a victim of its own success. Given that it is well ahead of any other hardware development of cryptographic protection and manufacturers are developing products, it appears that market forces have now taken over and there is no further role for government support.

The apparent success of AGA 12 obscures the additional work that is required. This includes several topics that—while of great importance to the success of the AGA 12 effort—are difficult to appreciate. These include the following:

- Conformance testing—While the AGA 12 standard will be validated by at least two National Laboratories, SCADA system owners and operators need a "seal of approval" to verify that the particular products they are considering buying actually do conform to AGA 12 requirements. There is no existing set of tests that is recognized as providing this assurance.
- Next generation design—Because AGA 12, Part 2 is a retrofit solution for legacy systems, it is the most expensive and least effective approach to the cryptographic protection to SCADA systems. Incorporating this protection into products at the time of manufacture is estimated to be less than half as costly as adding it after it is in the field. It is critical, also, that the next generation systems be able to interoperate with the units that have already had cryptography added.
- Large scale pilot test—While the laboratory and small-scale field tests that have been completed and will be done in the near future will validate that AGA 12 does work in the field, this is not a full scale pilot test. Several parts of AGA 12 that will function well during a small scale test may prove problematic for larger scale installations. Key management is a good example. Another is the possibility that network congestion problems might manifest themselves when many of the messages are encrypted, but will be invisible in small scale tests. SCADA operators are more likely to feel confident in a system that has been tested in a full-scale pilot than in a system that has only been tested on a small scale.
- Key management—Good cryptographic practice requires that the keys that decrypt the encrypted data and commands be changed periodically. This "key management" must be done remotely to be cost effective, since the wide geographic extent of SCADA systems prohibits visiting sites to change keys if a strike occurs or if an employee leaves.
- Forensics and diagnostics—While it is important that AGA 12 be able to protect SCADA systems from attack, it is also desirable that these systems detect attacks that are under way, inform the operator of the attack, and gather possible forensic information that will facilitate the detection, identification, arrest, and prosecution of system attackers. Although AGA 12 contains some features that lay foundations for this type of work, it is far from complete.
- Management port—The management port requires some additional features that are different from those required to send data and commands.
- Coordination of security standards—It is important that standards groups establish and maintain contact with one another. There are estimated to be approximately 100 groups currently developing cyber security related standards. There is very little contact among these groups, an undesirable situation likely to lead to duplication of effort and conflicting standards that no manufacturer will follow.
- High speed networks—While AGA 12's early focus on the protection of low speed legacy SCADA systems is appropriate in providing protection to the large installed base of these systems, it is also clear that many of the newer systems will use higher speed communication links, such as the Internet. This requires that we be able to maintain as much interoperability as possible between the low and high speed networks.

SEVERAL GOVERNMENT STEPS WILL ADVANCE SCADA SECURITY

In summary, we make the following recommendations

- Make sure that there is funding for R&D and strong industry-government partnerships to develop protection of the Nation's critical infrastructure against cyber attacks. Progress is being made—the key to moving forward is to continue R&D efforts and partnerships.
- Prevent loss of momentum by avoiding funding interruptions in on-going programs.

- Continue the coordination efforts (such as the DOE Control Systems Roadmap and the DHS Process Control Systems Forum) which are key elements of growing coordination between the government and industry and also vital to coordination among different infrastructures. These two programs are models for how to coordinate across a wide area.
- Support continued development of AGA 12. In particular, work should be completed to develop key management, establish conformance tests, do a large-scale pilot test, specify a next-generation design, secure high-speed networks in a manner compatible with the low speed networks, and develop forensics and diagnostics to detect and foil attacks.
- Support selected other standards development efforts. While our focus here has been on AGA 12, it is important to recall that this is only a small part of the total SCADA security requirements. Both the ISA SP99 and the NIST PCSRF efforts are noteworthy. Many of these other standards groups labor on an all volunteer basis on other critical requirements of significance as great as that of AGA 12. This all volunteer pace will not lead to rapid development of required standards.

Mr. Chairman, we applaud your focus on securing our critical infrastructure, especially in the area of SCADA protection. This concludes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittee may have.

LIST OF ACRONYMS

AGA—American Gas Association
AGA 12—American Gas Association Report No. 12, "Cryptographic Protection of SCADA Communications"
CM—Cryptographic Module
DOE—Department of Energy
EPRI—Electric Power Research Institute
GTI—Gas Technology Institute
ISA—Instrumentation, Systems and Automation Society
ISA SP 99—ISA Special Publication 99, "Manufacturing and Control Systems Security
NERC North American Electric Reliability Council
NIST—National Institute of Standards and Technology
PCSRF—Process Control Security Research Forum
RTU—Remote Terminal Unit
SCADA—Supervisory Control And Data Acquisition
SCM—SCADA Cryptographic Module
TNT—Tri-Nitro Toluene (dynamite)
TSWG—Technical Support Working Group, part of the Combating Terrorism Technology Support Office

FIGURES

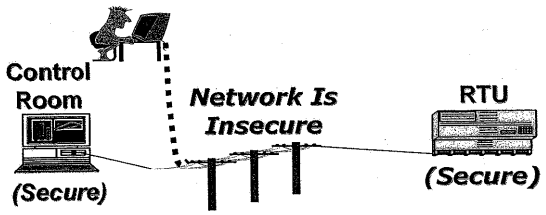


Figure 1 – AGA 12 assumes both the Control Room and the Remote Terminal Unit (containing the sensors and actuators) are secure

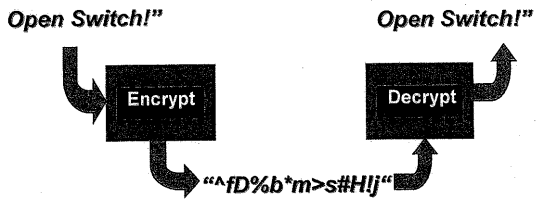


Figure 2 – AGA 12 specifies that the messages (Open Switch here) are encrypted inside a secure facility so that they are "scrambled" and can not be read. They are thus unreadable while they are on the insecure network, but can be decrypted and read properly when they are delivered to the second secure site.

Mr. LUNGREN. The Chair would now recognize Mr. Allan Paller, the Director of Research for the SANS Institute, to testify.

STATEMENT OF ALAN PALLER, DIRECTOR OF RESEARCH, THE SANS INSTITUTE

Mr. PALLER. Thank you, Mr. Chairman. SANS is different from the other organizations. We are basically an educational organization. We—our 45,000 alumni are the front lines, the people who put the security into the computers that try to block the attack. So we are constantly looking for methods that will make that feasible, because right now the bad guys are winning faster than the good guys are getting better.

So what I am going to do today is not talk about what the solution is to SCADA security, but how you can take—how we can prove you can take the solutions that Sam and K.P. and the others and Bill have found already and get them into operation rather than studying them to death. So that is what the testimony will be.

I do want to emphasize that you will sometimes hear these computers are not connected to the Internet; therefore, they are safe. The problem with that statement is they are often connected by packet radio. Think of old-fashioned wireless. So they might not be on the Internet, but the packet radio is the method by which the water treatment system in Maroochy Shire was taken over, and human waste backed up on the streets of the city, by a man who was angry at the system. It wasn't connected to the Internet, but it was very vulnerable. So we need to look at both of those attack methods. And these vulnerabilities aren't theoretical. You already heard them from Sam.

What I am going try to show you is a method and tell you a quick story of a method the U.S. Government has used that radically changed the dynamics of security in the country. And I think I will tell you that story and then finish this.

Microsoft systems are being put more and more into SCADA systems. You are buying them. GAO just came without a report that said that the problem—not just, a few months ago—came out with a report that says the problems in SCADA security are getting worse because they are connected to the Internet and because they are buying off-the-shelf, vulnerable operating systems.

So how do you make somebody who has a powerful monopoly over all of the computers that we buy change their way and deliver safer systems? About 2-1/2 years ago, the CIO at the Air Force got up at a public meeting and said, we are now spending more money to fix the problems we have because of Microsoft bugs than to buy the stuff in the first place. But he did something that no one else has done. He took Federal procurement power and said, we are going to fix this. And what he did is he consolidated all of the contracts that the Air Force has with Microsoft, all of them, and in doing that he saved $100 million. It is a half-a-billion-dollar procurement, but he has got provable savings of $100 million.

But that wasn't the exciting part of it. The exciting part of it was that he required Microsoft to deliver systems that were preconfigured according to the standards that DHS helped create, that the National Security Agency really fronted, and an organization called the Center for Internet Security brought together. So there was consensus benchmarks for what safe means, and that allowed the Air Force to require the vendor to deliver safer systems. It was a lot of argument, a lot of negotiation, but in the end Steve Vollmer and Microsoft said yes.

And what I am trying to show you is you can actually change the rate at which systems get safer by using combined buying power, and that is what I believe can be done very quickly in a SCADA environment, because what Bill is talking about, what Sam is talking about, what K.P. is talking about are actual solutions that aren't going to get implemented unless the buyers can act together, because the vendors—each individual vendor has an incentive not

to get ahead of the others because it will cost them more, and if they spend more, the other vendors can sell cheaper. So unless the buyers get together and agree on standards, it won't happen.

And what is exciting about the SCADA system is the State and local governments and the Federal Government have a huge concentration of them, so they can create an enormous buying power as long as the DHS and Sandia, and Bill and K.P. can agree on what those standards need to be. And it is a very quick thing. We are not talking about years and years. We are talking about weeks and months to agree on what needs to be done. But then instead of having regulations, instead of having laws, use procurement power to change things.

I thank you for allowing me to speak, and I look forward to questions. And I hope you feel better, Ms. Ranking Minority Member.

[The information follows:]

Testimony of

Alan Paller, Director of Research, The SANS Institute

Before the

House Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Hearings on SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems

October 18, 2005

Thank you for your leadership, Mr. Chairman and Madam Ranking Member, in shining a bright light on the insecurity of SCADA systems, illuminating the threat to the nation posed by their increasingly troublesome vulnerabilities.

My testimony today focuses on what can be done, quickly, economically and without new laws or regulations, to protect SCADA systems from attack. I'll do that in four steps:

1. Providing specific examples of the damage that has already been done by attacks on industrial control systems
2. Detailing why SCADA security is getting worse, not better.
3. Summarizing the available evidence on terrorist's use of cyber crime and how that can involve SCADA systems
4. Describing a promising and economical approach to improving SCADA security, an approach that has already been proven to work.

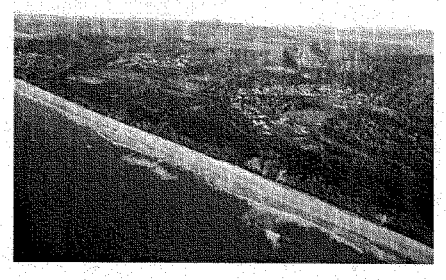
About the SANS Institute

The SANS Institute is the educational institution that prepares technical security professionals for positions of responsibility in protecting information systems. Our 47,000 alumni manage information security for commercial, government, and academic organizations throughout the world. At SANS they go through immersion training in intrusion detection, cyber forensics, perimeter protection, blocking hacker exploits, network and system security auditing, and security leadership. Courses range from foundational to the most advanced programs available anywhere in the world. SANS Institute faculty members exhibit two characteristics that set them apart from other security professionals: (1) They have the practical, in-the-trenches knowledge that makes their teaching credible. For example, SANS faculty have held positions as the Information Warfare Officer for the US Ballistic Missile Defense Organization, the internal Red Team Leader for the CIA, and the Technical Director for the Department of Defense Joint Task Force on Computer Network Operations. (2) They are the winners of an eleven-year competition designed to identify the best teachers in the security field. More than 700 people have tried out for positions on the SANS faculty; fewer than 30 have been selected.

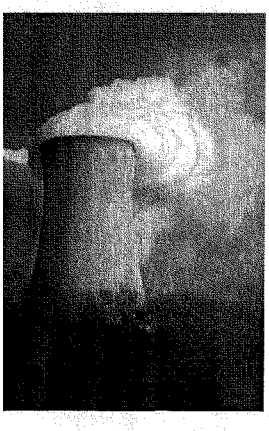
We also manage major research initiatives designed to enable our alumni to maintain their knowledge and skills after they complete SNAS training, and to help them protect their employers' information systems in the face of a constantly changing threat. For example, SANS operates the Internet Storm Center – the early warning system for the Internet with 6,000 sensors all over the world. It was Storm Center that discovered and illuminated the Leaves worm, the Lion worm, and the Katrina fund-raising web sites scams and it is Storm Center that security professionals look to every morning to learn what new attacks were launched overnight. SANS also publishes weekly security newsletters including summaries of all newly discovered security vulnerabilities with suggested solutions. That information is all available at no cost to our alumni and to every other person engaged in information security around the world. (www.sans.org)

Real Damage Has Resulted From SCADA Problems and Attacks

On October 31, 2001, Vitek Boden, an Australian, was sentenced to two years in prison for hacking into the SCADA system that controlled the sewage treatment plant in Maroochy Shire in Queensland, Australia.



Boden changed valve settings causing raw sewage to back up on the streets of the city, on the grounds of the local Hyatt Regency hotel (picture) and into the rivers. An Australian Environmental Protection official said, "Marine life died, the river turned black, the stench was unbearable for residents." And that was just sewage.



An event in January 2003 illustrated how accessible and vulnerable SCADA systems are at nuclear power plants, because they rely on vulnerable Microsoft operating systems, and why most utility executives are unaware of the risk. That month a computer worm, called SQL Slammer (SQL is a popular Microsoft data base management system), was circulating on the Internet. The Davis-Besse nuclear power plant, managed by FirstEnergy, had a firewall that blocked Internet traffic using SQL Slammer's path. Sadly, according to reports filed by FirstEnergy with the Nuclear Regulatory Commission (NRC), a Davis-Besse contractor had not protected that contractor's network. The worm came into the contractor's network, passed down a T1 communications line to the Davis-Besse computers without going through the firewall, and infected Davis-Besse business systems. Because of Davis-Besse's widespread use of vulnerable Microsoft software, the worm jumped to the plant network and crashed the Safety Parameter Display Systems, keeping it offline for eight hours. The report to NRC said "Some people in [First Energy's] Network Services department were aware of this T1 connection and some were not."

Because the Davis-Besse plant was offline and because it had back-up safety systems, this specific outage did not pose a major risk to public safety. However, the practices of using unprotected Windows operating systems and allowing contractors to bypass the firewall are common; many power plants and other elements of the critical infrastructure have similar vulnerabilities.

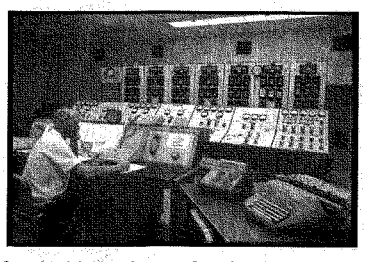
The bottom line is that real damage has already been done at some locations where SCADA systems are in use, and that the defenses SCADA operators have put in place can no longer be counted on to stop the attacks.

The Problem Is Getting Worse

In March 2004, the Government Accountability Office (GAO) published a report on SCADA security that it produced at the request of the House Committee on Government Reform Subcommittee on Technology and Information Policy. That report focused, in part, on why the risk to SCADA systems is increasing. It listed the four factors contributing to the escalation of risk to SCADA systems:

1. Control systems are adopting standardized technologies with known vulnerabilities. Essentially this means Microsoft software, UNIX and Linux software, and the Internet. The Davis-Besse example showed how reliance on Microsoft software and on the Internet enable malicious programs to take over utility control systems.
2. Control systems are connected to other networks that are not secure. This, too, was illustrated in the Davis-Besse outage, but we'll see an example of this in a moment.
3. Insecure connections exacerbate vulnerabilities. GAO focused on dial up connections, but the Davis-Besse worm attack illustrated that Internet connections are also insecure.
4. Manuals on how to use SCADA systems are publicly available to the terrorists as well as to legitimate users.

The event that first persuaded me that SCADA systems are directly vulnerable to terrorists and that real damage can be done, was documented in a book called @Large. It is ancient history now, having occurred in the early 1990s, but it is a perfect model for the attacks of today. It also helps explain the increasing vulnerability GAO described in its report.



Forty years ago, dam control rooms looked like the picture at the left, but over the next decades most of those manual systems were replaced by computerized control systems.

While this transition was taking place, particularly in the seventies and eighties, American's became aware of the possibility that terrorists could take control of the dams and open the spillway gates – flooding cities and killing people. Government officials, faced with the threat of such a catastrophic event, looked for a way to protect the citizens from such an attack.

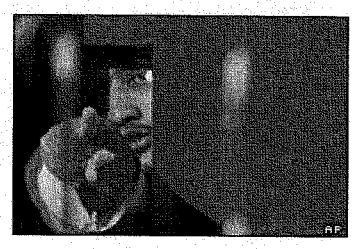
Computer networks were new and seemed promising. Some government officials decided to build communications links from their computers to the control systems at the dams so that officials could override any action a terrorist might take from inside the dam's control room.

Sadly, their actions created a new vulnerability much larger than the one they were trying to solve. Their error was documented by the authors of @Large. The authors described an FBI investigation of a hacker who had broken into many government systems. The lead FBI agent, Brent Rasmussen, discovered that the hacker had penetrated a Department of Interior network in Portland, OR, roamed that agency's national network, and skipped to Sacramento, "where he easily obtained root access on the computers that controlled every dam in the northern part of the state [of California]."

Root access means total control. The hacker could enter exactly the same override commands that the government planned to use to thwart terrorists. This particular hacker was just exploring every computer he could take over and had no knowledge of the dams he could control. The lack of effective security on the government systems and their ability to control the dam's spillways combine to offer a chilling roadmap for people who want to do harm to the United States.

So if the threat is real and it is getting worse, one must ask how and where terrorists can be expected to exploit these vulnerabilities.

Are Terrorists Using Cyber Crime?



Imam Samudra (picture) is the "first" Bali Bomber, the Al Qaeda chief who purchased and planted the bombs that killed more than 200 tourists in Bali in 2003. He was convicted and is now on death row.

Forensic analysis of Samudra's laptop uncovered evidence that the terrorist was involved in hacking for profit through credit card fraud. While on death row, Samudra wrote his autobiography and had it published by a commercial publisher in Indonesia. One of the chapters, called "Hacking, Why Not?" provided step-by-step guidance for his followers on how to become competent hackers and told his readers why he wanted Al Qaeda members to become hackers, saying,

> **"If hacking is successful, get ready to gain windfall income for just 3 to 6 hours of work, greater than the income a policeman earns in 6 months of work. But, please do not do that for money alone! I want to motivate the youth and Moslem men who are granted perfect mind by Allah; I want America and its cronies to be crushed in all aspects."**

Terrorist are getting better at hacking computers to raise money, and can be expected to add cyber extortion to their portfolio of crimes. SCADA systems can be a potent target for them.

Dave Thomas, chief of the FBI's Computer Intrusion Section, reports that the FBI is receiving more than one new case of cyber extortion every day. Criminals hack into computers and then threaten to expose or change information or disable the computers if the victims do not pay. Most victims are online businesses, but an extortion involving a computer that controlled a life-support system provides an example of cyber extortion more relevant to today's hearing.

In January 2003, a Romanian pair hacked into the computers at the Amundsen-Scott South Pole Station that controlled the life support for the 50 scientists there. The attackers demanded money. This attack suggests a future scenario in which a compromised SCADA system at a nuclear power station could lead to substantial extortion demands and more money for terrorism.

In sum, SCADA systems are vulnerable, their compromises have caused real damage and can cause much more, and the attackers don't have to be experts in SCADA operations to use SCADA compromises to extort money from operators of information systems controlling the critical infrastructure.

Is There A Cost-Effective Solution?

Surprisingly, there is an effective approach, that does not require regulation or legislation, and that has already been proven to be effective by the US Air Force. It recognizes the futility and waste of asking every buyer of SCADA technology to learn to reconfigure their SCADA systems for security, when the SCADA vendors can do that job one time and do it cost effectively. This approach employs the buying power of the users to persuade the vendors to do the work.. In the biggest example of the technique, the Air Force said to Microsoft, we will buy 525,000 Windows systems, if you are willing to sell them to us safely configured. Microsoft is to be applauded. The company said yes.

Procurement leverage is effective because it places the responsibility for securing systems in the only place that security tasks can be done cost effectively – in the hands of the system vendor that created the systems. The vendor is the only organization that knows the technology well enough to know how it can be secured, and the vendor can do it one time on behalf of all users. If, instead, you try to force every user to secure their systems, every user would have to study every system they buy and become a security expert on every system, and then they would do the same job the vendor could have done one time. Allowing vendors to foist the security configuration job onto their users is what got us into this vulnerable status. That's what has to change. That's what the Air Force changed by leveraging its Windows procurement. That's what government leadership can change by leveraging SCADA procurements.

The Air Force consolidated 38 contracts, creating a single, six year, $500 million procurement of Windows operating system and application software for 525,000 Air Force computers. Procurement consolidation allowed the Air Force to pay $100 million less than they would have paid had they not consolidated their buying. The main purpose of the procurement, however, was improved security. The Air Force required the software vendors to deliver Windows software pre-configured securely, so that every Air Force base didn't have to reconfigure it. Nearly every other buyer of Windows systems has to do the reconfiguration themselves, and few do it well.

The Air Force contract offers continuing savings and better long term security, because the standard configurations they are buying can be patched automatically and quickly. Automatic patching saves money. Quick patching protects Air Force systems from attacks other organizations face.

One critical element of the Air Force's procurement illuminates what DHS can do to improve security of SCADA systems. The Air Force had to have detailed security configuration standards to put in the Windows procurement. Without those specifications, there would be no standardization, and the entire secure Windows initiative would have faltered. The Air Force relied on secure configuration standards developed by the Center for Internet Security and the US National Security Agency.

What is not well known about the Air Force procurement was the role played by the Department of Homeland Security. DHS provided partial funding for the Center for Internet Security – the organization that created the consensus security specifications used in the Air Force procurement. The Center for Internet Security is a not-for-profit association of private and public technology users who combine their knowledge of security vulnerabilities in products they buy. The members of the Center build consensus specifications for securing more than a dozen common systems- including the operating systems commonly employed in modern SCADA systems. The Center's work is, in my opinion, the single greatest contribution DHS has made to meeting its published goal of reducing security vulnerabilities of the nation's critical cyber infrastructure. It is also the best example of a public-private partnership that actually improves security.

This same technique can be put to work in improving SCADA security and DHS has a central role.

First, DHS and the Center for Internet Security can bring together the SCADA vulnerability research that has been spearheaded by the extraordinary people at Sandia National Laboratory and the Idaho National Laboratory, with the experience of other users of SCADA equipment, to develop consensus safe configuration benchmarks for SCADA systems, very quickly. Once those configuration benchmarks are set, buyers of SCADA systems inside the government can incorporate those safe configuration benchmarks in their SCADA procurement documents. SCADA vendors that want their business will see their economic interest lies in meeting the requirement for safer SCADA systems. Non government buyers can also use the consensus specifications.

Sadly, what I just described, even if 100% successful, will still leave most of the critical infrastructure vulnerable for many years, because insecure SCADA system have very long lives. SCADA systems usually last ten to fifteen years and many last longer. To protect the legacy SCADA systems, a parallel technique can be used. SCADA vendors charge substantial maintenance fees, and buyers pay those fees. As part of the renegotiation of annual maintenance fees, the vendors can be persuaded to develop and deliver special network filters that isolate the legacy SCADA systems from other parts of the network – allowing only very specific information in very limited formats to get to or from the SCADA systems and to get to or from the systems that manage the SCADA systems. Only the SCADA vendors know what parts of the

network traffic are essential and what parts can be blocked. Here again, expertise from INEL and Sandia can help enable the process.

This second technique – filtering legacy systems – is the only known solution for securing old SCADA systems that use operating systems that cannot be patched and is a second layer of defense that can help protect even securely configured SCADA systems.

Here's the bottom line: We can improve security on SCADA systems quickly through DHS leadership and intelligent use of federal procurement. The costs are low; the value is high. We owe it to the country to try.

The Air Force demonstrates that safer systems can be acquired at very low additional costs. The vendors decided to comply because they wanted the $500 million dollars the Air Force would spend if they did. That $500 million (over 6 years) accounts for about one tenth of one percent of federal IT spending. Yet it has had a huge impact. Already Microsoft's Director of Security Engineering Strategy, Steve Lipner, told a Department of Energy cybersecurity conference audience in April 2005 that the next step for Microsoft, after the Air Force deal, is to "deliver the safer systems to all our customers."

If changing the specifications in one procurement, involving one tenth of one percent of the Federal IT budget could have that impact, think what can be done with a larger share of the IT budget. How many IT suppliers, including SCADA vendors, could be persuaded to deliver safer systems?

I greatly appreciate your allowing me to meet with you today and I look forward to your questions.

Mr. LUNGREN. I hope she feels better, too. I am not sure I feel better after hearing your testimony about the vulnerabilities that we have here.

We have now been informed that I guess we are to go back at 5:30, so we will have time to not only ask questions, but to hear your comments. And I appreciate your brevity, but I also appreciate the quality of the testimony.

This is a concern that many of us on this community have. It is, as someone said, the soft underbelly of our infrastructure, and it is something that doesn't immediately come to mind because we take for granted that we have these systems that work. And our increased interconnectivity is a blessing, but it is also a curse. It creates the vulnerability that makes that soft underbelly even greater. And I hope I am pronouncing your name correctly. Is it Dr. Varnado?

Mr. Varnado. Varnado.

Mr. LUNGREN. Varnado. I put the wrong emphasis on the syllable.

Dr. Varnado, of all the things that you suggested are our vulnerabilities, what would be the chief one; that is, the greatest—which would require the greater exertion of political will and governmental attention right now?

Mr. VARNADO. There are basically two approaches that we need to take. We need to continue to work on the inherent vulnerabilities that are there in every networked computer system. Industry and universities are doing a pretty good job in taking, looking at that one very hard.

The second area is that of induced vulnerabilities, something like what happened in Russia. And the problem with the COTS products, those are very complex systems. We have no idea what is deeply buried in those systems. The software that we purchase may have 20 million lines of code, and for us to reverse-engineer that is a very difficult task. Same thing with chips. There can be layers, seven, eight layers, in microelectronics today. More and more of those systems are embedded. So finding out how to reverse-engineer some of those products and to do security checks is a very difficult problem.

Now, the thing that comes to mind for Congress is trying to improve our collaboration among universities and industry and national labs and the government. There are things that get in the way, like classification issues. There are certain things about the threat that we can't talk about in this room. There are other issues like trust, antitrust, those kind of things, that the government could take some action to help give some relief in those areas so that we could discuss more. If we could discuss more openly the things that we all know, we would be in a better position.

So I probably didn't answer your question precisely, but

Mr. LUNGREN. Well, let me ask it another way. You said that—I mean, you almost articulated an insoluble problem which said we are attempting to build trusted systems with untrustworthy pieces. Other than us pulling in and saying everything we are going to do is going to be totally domestically engineered, produced, testing, et cetera, what do you suggest?

Mr. VARNADO. Doing it all ourselves is not in the cards. We can't afford it. So what we are doing is we are looking at different ways to configure systems that put security checks built into the technology as you assemble the system. So we are trying to decompose the system a bit and to put in security features where we think we might find problems and be able to detect problems quicker.

We do not have intrusion detection systems, for example, that operate in real time. That is why on the zero day exploits and the things like the 8 minutes of infecting the DOD system is so hard. We don't have these real-time intrusion detection systems yet. So we are working on those kinds of things to try to solve this problem. We cannot afford to build everything, no question.

Mr. LUNGREN. Thank you, Dr. Varnado.

Mr. Purdy, I have had a chance to hear you before, and I am very impressed with the breadth of your knowledge and the obligations that you have at your job. Having heard Dr. Varnado articulate the problem, as well as several other of the members of the panel, how do you at Homeland Security attempt to try and deal with this challenge, because in some ways it is a matter of priorities; and also, how do we—it seems to me that there is more things you can do immediately by command within the government than you can do in the private sector. How do you differentiate between what you can do by command in the government versus what you can do by whatever means in the private sector?

Mr. PURDY. Well, that is a difficult question which I know is one of the reasons that you asked it, and the importance of trying to get a handle on these issues. But essentially Secretary Chertoff's approach of risk assessment and risk mitigation, which underlies our National Infrastructure Protection Plan, and our work in building the partnership between government and the private sector for information technology within the sector and across the sectors, that is a fundamental piece of our effort. But we have prioritized several risk mitigation efforts within that context. One is control systems we have talked about. Another very important one is software assurance, and a third is Internet disruption, trying to promote the survivability and resilience of the Internet.

The software assurance piece that Dr. Varnado talked about relates to a number of efforts going on that are coordinated. The Department of Defense has a major effort in the software assurance area that is closely coordinated with our own software assurance security program.

The two fundamental things in addition to the purchasing power issue that Allan Paller talked about which we are working very hard on is the development of best practices along the development cycle for software assurance. And it is developing tools so that we can go back and assess the software after the fact.

The foreign issue that Dr. Varnado talked about, we are working in the unclassified and in the classified space. I am working as the cochairman of the globalization of IT within the Committee on National Security Systems, where the 24 agencies are coordinated on the national security systems so we can address exactly the kind of issue that Dr. Varnado talked about, the insecurity of what is made overseas, but, in fact, our inability to be able to tell on what is made domestically as to whether software not only does what it

is supposed to, but to make sure it doesn't do other things; the coordinated effort among the partnership, among the national labs; the funding that DOE, DHS—some direct, as our 15 million that is up this year for 2006—the money that our Science and Technology Directorate is funding; the additional funding that is provided for next year that goes to the I3P program that Sandia is coordinating; and a number of the specific efforts we believe are going to in 2006 provide some real deliverables to help make folks safer. But it is going to continue to require the partnership among everybody here, the owners and operators and the security vendors, and it is a difficult and important challenge.

Mr. LUNGREN. The Chair recognizes Ms. Sanchez for 5 minutes.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. Varnado, I wasn't going to ask a question, but you have me a little curious. When you talked about new systems and then intercepting them, did you mean like a little systems test as a piece of that hardware got made, or—I am trying to understand what you meant as an ability to counteract.

Mr. VARNADO. Right. What we are thinking, this is very much right now, Congresswoman, an R&D project that we are looking at. If we purchase most of the system and then we put it together, there are places in the data flow within the computer system that we may be able to put some small components in that would detect certain anomalies or violate certain patterns of use that would alert us more quickly and maybe even be able to prevent that from happening. So it is very much an R&D project at this point, and we are just starting to work on it the last 6 months or so. It is brand new. We think it holds some promise, but it is a huge problem, and we need to put more effort on it, I guess is the message I want to leave with you.

Ms. SANCHEZ. Thank you, Doctor.

Mr. Chairman, I am going to give up my time so that—because you have a lot of Members on my side who showed up to this, which goes to show just how important most of us think this is. And I am going to yield back the rest of my time and move it on.

Mr. LUNGREN. I thank the gentlewoman for yielding back and recognize the Chairman of the subcommittee Mr. Reichert for 5 minutes.

Mr. REICHERT. Thank you, Mr. Chairman.

Well, I am going to be totally honest. I am coming at this from a novice's perspective, and so I listened to you. My background is law enforcement. And so GTI, SCADA, NSTB, SCSC, NERC, AGA 12, cryptographic module and TSWG, and I had some more but I will stop. So, book them, Dano, is where I come from.

I am just really curious, you know, we need to be prepared. First of all, where are we really today; in your analysis of where we actually stand today, where are we? Anybody.

Mr. PALLER. The demonstrations of vulnerability are active and scary. So if you want to break into the power systems and the other systems in the United States, you can hire a bunch of companies that will demonstrate that it can be done. I just don't believe that we are at risk of that right away because it is easier to bring conventional weapons in and blow things up than to figure out exactly how to use that to blow up a pipeline. But I don't think we

are far away from it, and if we wait until we see the first strong use of it, there will be no catching up.

So it is hard to fix a problem when you don't see the attacks. It is very hard to spend money on that. That is why I like the Air Force method, because they actually didn't spend new money. They used old money and the buying power of the old money to make the change. I don't think there is another way to do it. There is not on lot of fresh money coming from the Federal Government.

Mr. REICHERT. Thank you. I thought that might be the answer.

And so when you look at what we need to do to become more responsive and aware, there is an educational training process that has to take place, not only some of the things that you mention in constructing the right system, but people learning all of the acronyms that I just mentioned, and I am sure there are a lot more. But how does local—how does the local government officials, how do they play into that, local law enforcement and also the local businesses?

You touched a little bit upon the industry and how they play a partnership, but when it comes to training, I think, Mr. Purdy, you mentioned training, and, Dr. Ananth, you said something about training 350 people. What kind of training, and who do you train?

Mr. ANANTH. Well, if I might say, the training that we talk about is for the people who install those control systems and for the end user. We are not talking about training the State and local people, because, as you know, sir, there is a lot of problem in interoperability devices with the response workers and the emergency response workers. But what we are talking about is the people who actually own the critical infrastructure assets, which is a lot of the private sector. So we are talking about where the control systems are located, so they need to know where the vulnerabilities are, they need to do a fix. So when we talk about the training, and when I talk about the training, that is the audience, the target audience, I was talking about, the owners of these infrastructure assets.

Mr. REICHERT. Mr. Purdy, did you have any comment on the training?

Mr. PURDY. Well, we have a number of different levels of the awareness piece that was touched on. I believe the House passed today a resolution to support National Cybersecurity Awareness Month, which is October, which helps emphasize the importance of getting the cybersecurity important message out to consumers and small business and what folks need do about it.

In addition the training program, we work with the National Science Foundation on the Cyber Corps Program, because we want to encourage the number of well-trained cybersecurity professionals in the Federal workforce, and as part of training we have been partnering with the Department of Defense, because one of the big issues about whether the Federal Government has enough well-qualified people is, if you define all the jobs differently, it is impossible to do the gap analysis. So they have done the job task analysis of DOD, and we are going to try to leverage that across the Federal agencies.

Also we are partnering with the National Security Agency. In fact, we have a major conference tomorrow up in Baltimore with

the Centers of Academic Excellence, as we have been creating a common body of knowledge for those university centers of excellence to train the next generation of cybersecurity professionals and software developers to do a better job of what it is that they do.

Mr. REICHERT. Thank you, Mr. Chairman.

Mr. LUNGREN. Mr. Purdy, I might just mention your reference to the bill that we passed yesterday. It is a great analogy for where we are. We passed appreciation for this month in the middle of the month. Maybe it shows you how we have to catch up in this whole arena.

Mr. Pascrell is recognized for 5 minutes.

Mr. PASCRELL. Mr. Purdy, I want to start off with this question, and I would ask you to be very direct and specific. How many Department of Homeland Security employees are currently working on the SCADA control systems issues? How many people?

Mr. PURDY. We have two government employees and 35 full-time contractors.

Mr. PASCRELL. So there are only two people in the Department of Homeland Security, and listening to the vulnerabilities from you six gentleman, we have two employees, Federal employees, and we are contracting out most of this work, correct? Correct me if I am wrong so far.

Mr. PURDY. On the control systems piece. The other efforts we are doing will help protect the control systems owners and operators as well, and that is integral to it.

Mr. PASCRELL. Well, then, let me ask you this question. We saw in the recent hurricane, Hurricane Katrina, that the Federal Government was unprepared to respond to a large natural disaster. Today we have heard about the devastation that may be caused if a terrorist or a—or there is a natural disaster hits our control systems. Mr. Varnado, you made four very specific recommendations. Just last week there was a headline in the New York Times that said, U.S. Cybersecurity Due for FEMA-Like Calamity. Are we prepared for a cyberattack on our control systems, Mr. Purdy? And if a natural disaster hits our control systems, are we prepared to respond to it, in your estimation?

Mr. PURDY. Well, we believe we are prepared for a cyberattack, to respond to a cyberattack against the control systems. Our partner division within the Infrastructure Protection Office, Protective Security Division, is the best division to talk about the actual direct physical consequences of your question.

Mr. PASCRELL. So from your standpoint we are prepared.

Mr. PURDY. We have a high cyber risk in this area, but we are prepared to respond and mitigate an attack that might occur, yes, sir.

Mr. PASCRELL. Well, there is no need to get on the defensive. I have a right to ask the questions, and you have a right to deliberate before you answer me.

I am getting particularly annoyed—for the Chair, I am getting particularly annoyed with employees that come here from the Department of Homeland Security, the responses to this committee or any committee dealing with homeland security, and frankly, I am

tired of it because we are not prepared. You know it, and I know it.

And let me make some suggestions before I leave it for now. We know that there are vulnerabilities within these systems, and we know that these vulnerabilities are abundant, and we know that the threat of the terrorist attack against these systems is real. Those things we know, we agree on. So the Congress, it would seem to me, needs to engage in a robust analysis and oversight in this realm, Mr. Chairman. We need to help ensure the security of the various control systems that are used in critical infrastructure. And I am heartened that today two Homeland Security subcommittees are leading the charge.

A cyberattack on one of New Jersey's four nuclear power plants or 100 chemical sites, for example, has the potential to be absolutely devastating not only in terms of lives lost, but also in the regional and national economic structure it could bring forth. That is very serious, very serious business.

Back in 2002, the National Infrastructure Protection Center reported that a computer belonging to an individual who had links to Osama bin Laden contained programs that clearly showed the individual's interest in the structural engineering of various critical infrastructures. It indicated that al-Qa'ida members had sought information about the control systems which we are talking about here today, from the very from the many multiple Websites.

The NIPP, the National Infrastructure Protection Plan, was due in December of 2004. Mr. Chairman, please hear me on this. This is important. The American people, American public is being duped. That was supposed to be completed in December of 04. In February of 2005, we had an interim plan. It was issued, setting a deadline of November 05 for the final plan. Now, according to the GAO, the interim plan was incomplete in the first place. It lacked both national-level milestones and sector-specific security plans. The plan remains uncomplete to this day. We can't even get proposals ready in a timely manner.

This is unconscionable. There really is only one full-time employee staffed in the DHS that deals with national cybersecurity, and I am not going to accept as a Member, Ranking Member, Ranking Member, it doesn't matter, I am not going to accept folks coming before us and thinking that we don't do our homework. And we are saying—we are talking here about on a nonpartisan basis.

This is critical stuff. You have never met deadlines. You don't care about those deadlines, and I don't think you have the expertise to meet the deadlines. What do you know about that? And I have not heard anything to the contradiction to that statement either. And I am tired of it, and the American people are tired of it.

Natural disasters. We are not going to have 7 days to prepare for a terrorist. We are not going to have 7 days. I suggest that you look at, if you haven't already, Mr. Varnado's four recommendations. It is a start. It is not the total solution. There is no seamlessness in this battle, no perfect systems, but it is 4 years later, and we are no further down the line, Mr. Chairman.

Thank you for your tolerance

Mr. LUNGREN. The gentleman's time has expired.

Mr. Purdy, if you wish to respond, you may.

Mr. PURDY. I expect that when the National Infrastructure Protection Plan goes out early in the year, that the concerns raised in the GAO report will be well addressed. The work we have done in the National Cyber Security Division to implement our strategic plan in furtherance of the national strategy to secure cyberspace, we believe, has made concerted progress. It has been reflected in the additional funding we have been given.

We believe Secretary Chertoff believes in the importance of the cyber issue as part of the overall risk management framework that he has. We are proud of the progress we have made. We would be happy to brief the Congressman and his staff and other members of the committee on that substantial progress. I recognize that the cyber risk is substantial. We recognize it is substantial. We agree with the committee. We agree with the members of the panel on that issue. To the extent the forcefulness of my answers came across as being defensive, I apologize, but that is how forceful I am. Thank you, sir.

Mr. LUNGREN. Thank you.

Before I recognize Mr. Pearce, I might just say there has been some frustration exhibited by this panel for the failure of reports to be done in a timely fashion, and I think that has been on a bipartisan basis. There is no suggestion on my part that you are not trying to do your job, but I will just tell you that is a real frustration on this committee.

Mr. Pearce is recognized.

Mr. PEARCE. Thank you, Mr. Chairman. I have got several questions, so I am requesting briefer answers if you could.

Mr. Purdy, can you outline the process by which the four components, divisions of the Office of Infrastructure Protection coordinate and share information in the progress or implementation of your mission? You have got four divisions. How do you all coordinate and share information?

Mr. PURDY. You are talking about generally?

Mr. PEARCE. Generally, yes.

Mr. PURDY. Across the board, well, we have two meetings a week with the Assistant Secretary for Infrastructure Protection, each of the division directors. We have an additional meeting without the Assistant Secretary where the division directors themselves come together. We have milestones that come down from the Infrastructure Protection Office weekly. We have weekly reports that the Infrastructure Protection Office gives to each of the divisions so that people know what the other groups are doing. And we have a number of specific areas that we are partnered with; for example, the Protective Security Division, they do the site-assist visits of the localities, and we provide the cyber guidance for those assessments that are due in the local locations. In addition, we have periodic briefings, where each division briefs the entire group, all the division heads from Infrastructure Protection, as to what the goals, objectives, accomplishments, budgetary situations are, progress and challenges ahead

Mr. PEARCE. Mr. Todd, do you have—you have heard Mr. Purdy's discussion. In your report you talk about the need in the future for maybe coordinated contact with other agencies. In the past year

what contact have you had with Mr. Purdy's National Cyber Security Division?

Mr. TODD. Well, let me handle them in two different ways. One is the—

Mr. PEARCE. If you could just give me the brief answer. What contact have you had with them?

Mr. TODD. I have not had any with them.

Mr. PEARCE. Thank you.

Dr. Varnado, what contact has your group had?

Mr. VARNADO. We are currently working with him on the National SCADA Test Bed as well as a program at Dartmouth that we are interacting on.

Mr. PEARCE. Okay. Thank you.

Mr. Todd, as I read your report, I just find the language to be very reassuring, very reassuring, and I find the language of the other reports to be not so reassuring; that is, I hear pointed comments. In other words, you say that you all have made the appropriate improvement measures, engineering, that you have done what you can to protect the equipment and ensure the safety of public health, that you have maintained a policy of not connecting your SCADA systems. You have evaluated and improved, you have identified the cyber vulnerabilities. You are continuously evaluating. Now you list a couple of sections, but then your closing statement says that we believe our security program meets the challenges of these requirements, and then kind of a throwaway comment that we will look forward to contributing and just staying on top of the situation.

Do you find the reports of the other agencies, the other people testifying here today, to be that much different from your findings? In other words, I find some element of alarm in everyone else's, but yours declares that we are on top of it, and we have been on top of it, and we are going to stay on top of it.

Mr. TODD. Well, let me say it this way; the differences, I believe, are this—we are an agency that puts things out on the ground. So we are certainly vulnerable to the kinds of contractors and chips and so forth that we might contract for. That is true. However, in our implementing these kinds of SCADA systems, we have had, over the last 20 years, a basic distrust of the system itself. We want it to be foolproof. And so we have put in other kinds of guarding devices. For instance, we have operators on 24 hours a day. We check with transmission agencies continually about what is being provided and what isn't. And if those things are not right within our parameters—

Mr. PEARCE. You feel like you could fight off any attempts, like the Australian attempt that is reported by one of the other presenters, that that really would not happen in your agency, that there is not much attempt or much capability for an outside group to come in and affect the flow of waters through the BOR or through the dam system or—you know, you think that you really are that secure.

Mr. TODD. We believe the risk is low.

Mr. PEARCE. Okay. Thank you. Appreciate it, Mr. Chairman.

Mr. LUNGREN. I thank the gentleman.

As I understand it, you do not have the SCADA systems running the gates; is that correct?

Mr. TODD. We do not have SCADA systems running spillway gates. We certainly have them running the smaller power gates for power generation, that is true.

Mr. LUNGREN. But the greater danger is with the spillway gates.

Mr. TODD. Yes, it is. Our SCADA systems are set to operate within the safe channel capacity, and so, therefore, we do not have them hooked up to the spillway gates, which are set to operate sometimes out of the channel capacity.

Mr. LUNGREN. I thank the gentleman.

Mr. LUNGREN. It is my pleasure to recognize the chairman of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you. I am interested to know from Mr. Pearce's answer that it was low risk. And the chairman just asked the question—you said, it was high risk; if I could get clarification and communication from one to the other, with the dams.

Mr. TODD. Excuse me, I am not quite understanding the difference of what you are asking.

Mr. LUNGREN. Mr. Chairman, I was asking about—the highest risk, as I understand it, comes from the control of the gates from the spillways and they are not on a SCADA system. Even though they have a SCADA system that does deal with the gates that go to the power plants, it deals with the volume, so the highest risk.

Mr. TODD. Okay, I think I understand what you are asking. Our SCADA systems operate power plants, and in those power generation plants they have turbines which—we have special inlets which have some gates to those turbines. Those are much smaller systems that, if all were turned on, for instance, full speed, they would still operate within the channel capacity downstream, so it wouldn't cause a catastrophe or consequences of damage and that sort of thing.

However, we also, in operating the dam, have much larger gates because of high flooding and other kinds of events that we have to safeguard the dam itself. Those gates, which if operated at full capacity, might go out of the channel capacity; those gates are not hooked up to the SCADA systems. So our SCADA systems would only operate within the safe channel capacity, itself, of the river.

Mr. THOMPSON. Is there a plan to put them on the system?

Mr. TODD. Not that I am aware of.

Mr. THOMPSON. Mr. Purdy, the President asked in 2003 that we put together this National Infrastructure Protection Plan. As you know, we have more or less missed deadlines, and when we finally got it, GAO was very critical of the product. It was pulled back, and I would assume that at some point we will have another response or report put together.

Do you have any idea when we will have that?

Mr. PURDY. Well, I will expect the report to come out shortly after the first of the year. Once that report comes out, then the sector-specific plan—such as, our sector is information technology—there will be a 6-month period in which we work with the private sector to create those plans.

So the specific implementation plans in each sector will be ready 6 months after that.

Mr. THOMPSON. So we will miss the November deadline?

Mr. PURDY. Well, I will leave that up to my boss, the Assistant Secretary, to—I believe he is coming to the Hill on Thursday. So I probably shouldn't officially comment on meeting that deadline, but I am confident it will be there shortly after the first of the year.

Mr. THOMPSON. Okay. All right.

Well, Mr. Chairman, I hope you noticed that we are still a little tardy with our deadline.

Mr. LUNGREN. I understand that. I also apologize for calling you chairman. Either—

Mr. THOMPSON. No, I accept.

Mr. LUNGREN. Either I have granted Ms. Pelosi's fondest wish or I have inducted you into the Republican Hall of Fame, so whichever one you would like.

Mr. THOMPSON. Well, okay, either way, I accept.

The other thing, Mr. Purdy, I am a little concerned about is the fact that we don't have but two full-time employees in your Department; is that correct?

Mr. PURDY. We have two Federal employees working on the control systems area and 35 contractors. We have an allocation of 40.

Mr. THOMPSON. Explain the contractors to me.

Mr. PURDY. They are people paid—many of them are through the national labs, for example, people that are not official government employees that are paid on a contract basis through a contractor. That is supporting our efforts in the control systems area. My division is the National Cyber Security Division which—control systems is one part of a broader effort.

So we have an allocation of 40 Federal employees. Of those, we have two and one to be hired for the control systems area that are official government employees.

Mr. THOMPSON. Now, the contractors, are those individuals that are contracted?

Mr. PURDY. No, they are through companies or through the national labs.

Mr. THOMPSON. All right.

Can you provide this committee with how much that is costing taxpayers, rather than having full-time employees, how much we are paying those contract employees?

Mr. PURDY. Yes. We can get you how the funding is broken down by contractors, yes, sir. We can get you that.

Mr. THOMPSON. For the record, can you tell me whether or not we are paying more for those people based on contracts than if they were full-time employees?

Mr. PURDY. I can't. I haven't seen the per-person breakdown of it. So I can't answer that question, sir, but we will be able to give you information from which that will be obvious.

Mr. THOMPSON. Well, just tell me what your best guess is. You are over it, right?

Mr. PURDY. I couldn't hear you.

Mr. THOMPSON. You are over it, right, you are over the division?

Mr. PURDY. Yes.

Mr. THOMPSON. You approve the contracts?

Mr. PURDY. Yes.

Mr. THOMPSON. Well, just give me a best guess whether we pay more for the contract employees rather than if they were on a Federal payroll.

Mr. PURDY. My best guess is, we are paying more for contract employees, yes, sir.

Mr. THOMPSON. How much more?

Mr. PURDY. Sir, that really would be a guess. I really shouldn't venture there.

Mr. THOMPSON. Well, so is it your opinion that we get a better product with contract employees than full-time employees?

Mr. PURDY. I am given a certain allocation of Federal employees to achieve our mission and implement our objectives and goals. So to do that, we need to hire contractors to help us fulfill our mission.

Mr. THOMPSON. So, in other words, you can't hire but three people?

Mr. PURDY. We can't hire but 40 people, right.

Mr. THOMPSON. Out of that 40, you chose to hire three in the Federal system and then contract everyone else?

Mr. PURDY. That is correct.

Mr. THOMPSON. Even though it costs us more to contract, there are 37 others?

Mr. PURDY. Yes, sir.

Mr. THOMPSON. Well, I guess when you have got a lot of money, you can do that.

Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you, Mr. Thompson, Ranking Member Thompson.

Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you very much, Mr. Chairman.

Perhaps as a follow-up to Mr. Thompson's question, if these are individuals and you have a contract with them, you obviously have a deliverable. What are they supposed to be delivering?

Mr. PURDY. I am sorry.

What are the deliverables? Maybe that would help us to understand, when you do respond to the question, if you would also put what the deliverables are, because it could very well be that there isn't any qualified employee.

I think, in addition to the deliverables, a natural follow-up question is, what is the length of their contract and when are they supposed to produce and what are they supposed to produce? I think that would be very appropriate.

I know you probably don't have that with you now. But in addition to how much are we spending, I think that that is an important follow-up component.

The SCADA system is something that I was familiar with. I used to be a contracts manager at a water management district, which meant I got to okay the payments, the monthly and quarterly payments for the SCADA systems, for their structures, their control structures. So, naturally there is a concern, you want to make sure that they work. But that was long before 9/11, so when you look at all the other systems, obviously the whole SCADA system of controls is just very, very important.

While we have concentrated on how many employees work for you on SCADA, maybe we also need to ask, do you know how many are at NCSD?

Mr. PURDY. Well, as I said, we have an allocation of 40. We have 25 or 26 in place. I believe we have six or seven in the hiring pipeline; we are pursuing hiring an additional balance of the 40.

Ms. BROWN-WAITE. Okay, and in a follow-up question, what is the plan for the NCSD in the reorganization?

Mr. PURDY. Our division will move, of course, into the larger preparedness directorate, the information analysis, infrastructure protection directorate; that is, the Under Secretary level has become a preparedness directorate.

Within that, we will move along with the telecommunications folks, called NCS, National Communications System. So cyber and telecommunications will be under a new position that is being created for an assistant secretary for cyber and security telecommunications. So we will be under a new assistant secretary who will, in turn, be under the under secretary for preparedness.

Ms. BROWN-WAITE. I can tell you that so many constituents just feel that the Department of homeland Security is nothing other than bureaucracy, layer upon layer, and that there is just a lot of concern out there that the major question is, are we safer for it today.

Can you also tell me, Mr. Purdy, what progress is actually being made in developing standards for SCADA systems?

Mr. PURDY. Well, some of the members of the national labs here can probably go into more detail than I can. But within the framework of our plan for 2006, there was some discussion about the cyber security protection framework to develop and disseminate tools to assist the users in assessing their cyber security practices against industry best practices and standards. We are trying to work to perform those vulnerability assessments to identify the weaknesses in the systems against those standards and recommend mitigative strategies for them.

The Process Control Systems Forum, which we cosponsor with the Science and Technology Directorate, with the users—again, we are working with the owners and operators, the vendors and the national labs to help identify the specific standards for the control systems against which we can judge how the actual owners and operators are doing.

Ms. BROWN-WAITE. So I think what you said is, there is no standard yet, but you are working on it. Is that—

Mr. PURDY. We have a draft cyber security framework, as I said in my testimony, that we are going to be piloting this year, that we will then be able to roll out this year—"this year" being 2006—so that the individual companies can do their assessments. That is going to be part of the effort as discussed by others to build the business case to convince the owners and operators to spend the money to meet the standards.

Ms. BROWN-WAITE. Do you believe that there is a way that government can incentivize the private sector to actually develop smarter SCADA security?

Mr. PURDY. Well, within the context of software and in controlled systems, we want to do—and we have begun to do what Alan

Paller was talking about, which is put in incentivizing programs for those contracts which the Federal Government is buying so that we can raise the bar in a nonmandatory way—not like in a regulatory way, but if you want to get the contract, you have to have the security built into the system you are selling. We believe that is an important basis.

In addition, having the assessments and the framework and the tools for self-assessment, that is going to help encourage and make the business case for the private sector to spend the money.

Ms. BROWN-WAITE. Thank you, Mr. Purdy.

I yield back my time. I thank the chairman.

Mr. LUNGREN. I thank the gentlelady.

The gentlelady, Ms. Norton, is recognized for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman. Actually, it is this latter point, and I was going to direct the question to Mr. Paller, because I was intrigued with his notion of requirements of the contractor essentially to deliver security-ready systems.

It seems so obvious that I have to ask you—it seems obvious because, obviously, if you are delivering to the big granddaddy of them all, the Federal Government, you really do call the shots. You know, it is like Texas calling the shots on textbooks that everybody else has got to use, because they have more kids. Or it is like Medicaid prescription drugs, where we ought to be taking advantage of our market advantage. This goes to the underlying substance: Who in the hell needs this more than the Federal Government?

What are the—I mean, what do we—what are the barriers? I mean, for example, is this very costly to do? If so, you know, I can't imagine that it would cost us even more to do it after we got it. So that is one question.

Are there security reasons? Is there some discussion of contractors and whether or not you want them that much, excuse me, in on your business, but they, of course, I presume, know all this in the first place.

I would like to know what are the real barriers to this and whether it can be done, because you indicated it can be done pretty quickly.

Mr. PALLER. There are two barriers that we have seen, one—and they are both real, so that when people fight against it, they are fighting not irrationally.

One is, if you take responsibility for securing systems and you deliver a more secure system, when the user wants to do something that is not turned on by default, he may call up for support. So there is a support issue that comes in.

But the much larger one, that the lawyers get involved in, is that they are worried about taking liability. They are concerned that if they say, now we are going to give you a more secure system, that somehow the trial lawyers will be all around them. At least that is what they say.

But could I just take one second and answer another question that I wasn't asked?

Ms. NORTON. On my time?

Mr. PALLER. Yes.

Ms. NORTON. No. Because I have another question.

Mr. PALLER. All right. You.

Mr. LUNGREN. Normally, we would allow you, but we have a short time frame here.

Ms. NORTON. If he would have extended my time—see, he is not going to do that.

I have got to go to Mr. Purdy and ask him about the four cyber security managers in so short a period of time, high turnover, and of all positions, the security managers at DHS. As I understand it, the last turnover was in January. This doesn't make me feel very secure.

Mr. Purdy, I would like to know why there is such turnover in the cyber security managers, what you can do to correct it. I can't believe it is good for the system.

I want to know what the effect is on cyber security, and I want to know why the Secretary hasn't appointed a new cyber security manager here in the month of October?

Mr. PURDY. Well, let me address the last question first. It is certainly my expectation and hope that now that the new directorate is stood up by the President signing the Department of Homeland Security budget, that Secretary Chertoff will announce the appointment of an assistant secretary for cyber security and intelligence.

Ms. NORTON. Excuse me, so you are saying it was a budget question?

Mr. PURDY. The position did not exist before the President signed the budget. All I am saying is, it is my expectation.

Ms. NORTON. I thought there were four cyber security managers. So you are saying the position of cyber security managers did not exist?

Mr. PURDY. I am sorry. I am trying to answer your last question first, the question on Secretary Chertoff appointing a new assistant secretary for cyber security and telecommunication. And I was saying, it is my hope and expectation that he will make that appointment very soon now that the new directorate has been stood up.

I think the publicity about high-level departures from my division is really overblown. To me, the progress that we made from the time I came over from the White House, having worked on the national strategy, in April of 2003, through the time when Amit Yoran, my predecessor, was in office and some of the other folks have left and are gone, we have built and have implemented a very important complex plan to reduce our cyber risk. We do not believe that has been impacted by individuals' departing.

Ms. NORTON. Why are they departing? Please answer my question; I have limited time.

If there have been these rapid departures, one, why have they departed; and two, what can we do to keep turnover in all divisions of cyber security managers? I would like to ask my question because, you know, everybody is going to leave here in a minute.

Mr. PURDY. Some of the positions were departures based on personal reasons that were not related to mission. I think that is primarily what we are talking about, not related to mission.

We believe we have the positions in place. We have the plan in place. We have the funding, particularly with the additional 2006 money, that we are going to be able to keep strong people, and we are going to be able to implement our strategic plan.

Ms. NORTON. I will accept that as a promise.

Thank you, Mr. Chairman.

Mr. LUNGREN. I thank the gentlelady.

Ms. Jackson-Lee is recognized for 5 minutes.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman, and to the ranking member. We don't have a lot of time for what I think is a very important hearing.

I guess I remain troubled by, one—Mr. Purdy, maybe you can tell me, you might be under review or under the consent process of the Senate. You might advise me of that. But I continue to be troubled by the acting director scenario, because I think in the Department of Homeland Security we are rattled, if you will, with interim and acting personnel when we have a very serious challenge. So I know in the course of your response, you will provide me with that.

I would like, first of all, to ask unanimous consent to have my statement submitted into the record, Mr. Chairman.

Mr. LUNGREN. It is so submitted.

Ms. JACKSON-LEE. But what I would like you to walk me through again, and if you have said this previously, thank you for repeating it in a more detailed manner, and that is the absence of a National Infrastructure Protection Plan. Why don't you tell me why no such plan exists?

I am sure you are going to tell me that it is either being worked on or it has been submitted, and I missed it. But then also tell me what you would expect to see in such a plan?

Let me just highlight for you that in the course of at least 6 months, we have had a number of incidents at our chemical plants and refineries in the gulf coast region. Adding to the misery, of course, were Hurricane Katrina and Rita in terms of control data systems determining the status of those particular entities, one, the vulnerability to terrorism and other catastrophes that might make the situation worse.

So obviously this hearing is extremely important, because we are talking about control systems and SCADA systems which are sometimes confused and intermingled.

I think it is obviously a failure that we have never finished our national vulnerability assessment or national threat assessment that I think many of us have been asking for for a number of years now, since 9/11.

Now I understand that we don't have the particular National Infrastructure Protection Plan relevant to the issues at hand. Would you, first of all, respond to—you could give me your status, but would you both tell me whether there is an existing plan, but then what you would expect or would see, expect to see, in such a plan to be presented and to be in place?

Mr. Purdy.

Mr. PURDY. So the existing status, you are talking about my acting director position?

Ms. JACKSON-LEE. I am. Are you acting or are you in the middle of being confirmed?

Mr. PURDY. No.

Ms. JACKSON-LEE. Or what is your stance?

Mr. PURDY. No. I am the Acting Director of the National Cyber Security Division, and we are waiting for the appointment of an assistant secretary for cyber security and telecommunications, who

will be my boss; and he or she will make the decision of whether I will be director or in some other position.

Ms. JACKSON-LEE. So we are in complete disarray?

Mr. PURDY. No, I think we are implementing our strategic plan in furtherance of the National Strategy to Secure Cyberspace. I think we are making demonstrable progress, and we are happy to brief you in more detail on it.

Ms. JACKSON-LEE. Can you help me then with the question that I asked, why do we not have such a plan right now?

Mr. PURDY. The responsibility for the plan is the responsibility of my boss, the Assistant Secretary.

Ms. JACKSON-LEE. Who doesn't exist at this time?

Mr. PURDY. The Assistant Secretary for Infrastructure Protection, until the time that President Bush signed the budget, was my boss. When the budget is signed, as soon as my bosses tell me that there is a change, then there is a vacancy creating an assistant secretary for cyber security and telecommunications who will be my boss. So we are in a little bit of a transition period.

But in response to your question, they didn't want to make a decision to drop the "Acting" from my title, giving the opportunity to the person who will be my boss, so that he or she can decide who they want in that position and how they want to organize cyber security and telecommunications in a cohesive and integrated way.

Ms. JACKSON-LEE. Let me acknowledge that I am putting you in probably an untenable and embarrassing and compromising position in terms of trying to answer the question. Let me thank you, first of all, for your service, but let me admit that what you have just said sounded as convoluted as one might imagine.

It is almost incomprehensible what you just said. I think I gleaned from it that someone that was in the position went on to something else, and they are dealing with the budget, and therefore, we are not in order.

I would only say to you this: The acts of terror really don't make appointments, and they don't respond to our lack of personnel in place. So your response certainly is not your responsibility and fault. But let me go on record and say that we are in disarray, and we are dangerously in disarray in a very important area.

I do acknowledge that recent legislation had funding in the cyber security area, and I am very glad of that, and amendments that we have put forward have been accepted, but still—would you please answer the question again?

I don't think we will agree on whether or not the area where you are in is in order, but can we at least agree, is there or is there not a National Infrastructure Protection Plan, yes or no; and if there is not, prospectively what would you expect to be included in that plan?

Mr. PURDY. The draft of the National Infrastructure Protection Plan is on Secretary Chertoff's desk, and we expect it to be circulated for additional comment in the next few weeks.

Mr. LUNGREN. The gentlelady's time has expired.

Ms. JACKSON-LEE. I thank the chairman.

Mr. LUNGREN. The gentleman from North Carolina, Mr. Etheridge, is recognized for 5 minutes.

Mr. ETHERIDGE.7 Thank you, Mr. Chairman.

Mr. Purdy, at the risk of embarrassment, I am going to go back to the issue that we are still on, and then I have—I am going to move on and try to get to another question.

As you draft the response to this question on the budget that you had indicated you will share with us relative to the 40 slots that are available in your area, I recognize that you are only the Acting Director. But that doesn't matter; this committee deserves the information.

I would like to know, and I think the other members of the committee would like to know, as you look at that, since we only have three permanent positions, what—as you draft the numbers for the cost of the contractors, how much the taxpayers of this country would be saving if we had full-time positions and what the turnover would be if they were not contractors that moved back and forth.

I think it is critical—and I am going not going to ask you to answer that today, but I think it is a critical issue to have permanent people you can have access to, that can be trained, who aren't likely to have the information and you have to move on and you have to have different people in place. I think that has a real impact on continuity.

Because you said early on that cyber security is important. I happen to believe it is, and if it is important, it ought to be important enough to have permanent, full-time people to be there in place on a daily basis to deal with these issues that are important to the taxpayers of this country and to the people of America.

I hope you agree with that.

Mr. PURDY. Yes, sir.

Mr. ETHERIDGE. I hope you will add that to the material you are going to send us.

Now, my question is this: I wanted to follow up, and you probably can't answer it, because you have tried to get to it and haven't really answered it thus far, simply because I think it is above your pay grade, and that is inappropriate, because having as many people in this position since the Department has been funded creates a real problem of continuity for people now, in this period of time, without having someone permanent.

I am going to leave that out there and not ask you to respond to it, because I think it is inappropriate to ask you to respond to it. But I trust this information will get back to the Department. Hopefully, the Secretary will be here at some point, and we will have an opportunity to ask that question.

My question to you and to Dr. Rush and Mr. Paller—I will say this: The Department of Homeland Security established the Process Control Systems Forum to facilitate communication between government, industry, vendors and academia. Are you familiar with that?

Okay.

How effective has this endeavor been, and do you know of any meetings between these groups? If you do, what was the outcome?

Mr. RUSH. Yes. I would say those are some of the most effective activities I have seen.

We are developing standards; we are feeding them in. There are two activities—well, really three, but the two that you mentioned,

the PCSF, the Process Control Systems Forum has brought together the vendors, the manufacturers, the users, cryptographic experts, the whole field. That has been very effective.

There was a question about coordinating Chairs. We had a meeting just a couple of weeks ago where there were literally dozens of organizations getting together and swapping glossaries and making substantial progress.

Mr. ETHERIDGE. Beyond philosophies, though, did we get any results?

Mr. RUSH. Absolutely.

Mr. ETHERIDGE. Can you name, share with us some of the results?

Mr. RUSH. In terms of things that are out there?

Mr. ETHERIDGE. Yes, please.

Mr. RUSH. Here is a product that conforms to one of the standards. What you need to understand is the standards groups are volunteer organizations, and they don't have the resources to coordinate. This provides them with exactly the forum that they need to exchange. We have got 100 groups working independently. Imagine 100 congressional committees not talking to each other.

Mr. ETHERIDGE. Good. Thank you.

Mr. PALLER. Yes. It is a wonderful talking group. Bill's outcome is very real. There is a problem with groups like that. It was seen in the health—the security of the health devices, CAT scanners and things like that.

When the vendors have too big a role, implementation of security is delayed almost endlessly. So at some point, the users have to say, this is our need, our things are at risk. Vendors are going to have to deliver what we say rather than letting the vendors hold it up.

So PCSF is the best thing out there, but at some point the vendors will have to be asked to wait outside while they vote.

Mr. ETHERIDGE. Mr. Purdy.

Mr. PURDY. In addition, the PCSF has provided the input that has led to the development of the security framework, which helped set the best practices and also provided the input for the development of the assessment tool. The assessment tool, which is now being used to test, is used to assess the cyber components of the control systems and then provide the checklist and the questionnaire to determine the particular vulnerabilities and whether the mitigated steps have been put in place. That collaborative effort is what is helping to drive solutions to a very complex problem.

One of the reasons for the complexity is that so many different owners and operators have so many different systems with different levels of maturity. So it is hard to have one set fix across the board to make it better. So that is why the collaboration in developing these tools in the framework has been so important.

Mr. ETHERIDGE. Thank you. I yield back.

Mr. LUNGREN. The gentlelady from the Virgin Islands, Mrs. Christensen, is recognized for 5 minutes.

Mrs. CHRISTENSEN. Thanks, Mr. Chairman. Let me ask a little bit different question.

I want to ask Mr. Paller about the training, because that is your responsibility also, the training of the technical security profes-

sionals. Where are we, how many have you trained? What is our need? How are we meeting that need?

Also, where did the students come from? And do you work with universities, and if you work with universities, to what extent are minority-serving institutions involved?

Mr. PALLER. When we get all done training everybody we can train, we won't have touched 1 percent of the people who have control of these systems. So the solution is not to train more people. We have got to build safer systems; then the training will have an effect. So as hard as we work, we will never get there.

I do want to go back to Mr. Reichert's question. We actually work with universities and local law enforcement. They don't have the funds that large companies do, so we have major programs where we cut the costs of education by about 85 percent, so they get a much lower cost. So locally we work with the FBI to set up these programs for local law enforcement. It actually is wonderful, because they give more feedback, and they are the best students we get.

But the training of the SCADA people, we have just begun with courses on how you measure SCADA security, and they are just starting. I think the jury is still out. You have got two groups. You have SCADA engineers on the one side and security people on the other side, and getting the course right for those two interest groups is challenging. So we will know in the spring how that works. .

Mrs. CHRISTENSEN. Okay, just one other question for

Mr. TODD. Since I sit on the Resources Committee, I am glad to know that your SCADA system is not connected to the administrative systems because that is one of the problems we are reading about.

Do you monitor only the 17 dams that the Bureau has created or are you monitoring the private dams? Have you used the RAM–D to assess the threats, vulnerabilities and consequences; and to what extent are the dams that you are assessing, how far along are you?

Mr. TODD. We—of course, as you said, we don't have any responsibility for the non-Federal dams. But in reclamation, we have 252 high and significant hazard facilities, and of those facilities, we have assessed all of them. What we would call our "major mission-critical facilities," which are the very top-producing power-generating dams and also very high dams, we have used the RAM–D on. There are about 50 of those that we used the RAM–D that was developed in conjunction with Sandia. Those are assessed, and those are the ones that we did.

Now we have used the other ones. We have done different priority dams and low-cost methods.

Mrs. CHRISTENSEN. I yield back my time.

Mr. LUNGREN. I thank the gentlelady for yielding.

Mr. Dicks is recognized for 5 minutes.

Mr. DICKS. I wanted to go to the dams question. It says here, significant information on control systems is publicly available. It says design and maintenance documents, technical standards for the interconnection of control systems and standards for communication among control systems, all of which could assist hackers in un-

derstanding the system and how to attack them. Moreover, there are numerous former employees, vendors, supporters, contractors and others, end users of the same equipment, worldwide, who have inside knowledge about the operation of the control systems.

So, Mr. Todd—and we have got information here that al-Qa'ida has, in fact, said they are interested in the operation of these dams. I am told—maybe you covered this earlier, but I have got to go back to it.

We have heard the story of a hacker gaining control of some systems of the Roosevelt Dam in Arizona, which holds 400 trillion gallons of water. What is the worst damage that could have been done there?

Mr. TODD. In that particular situation—and that happened a number of years ago and, of course, there have been a lot of upgrades to that system to not allow that to happen again; that individual did intrude, but did not get access or gain access to any of the operation of the gates and so forth.

Mr. DICKS. Could it be done from outside?

Mr. TODD. Well, yes, there are always those possibilities that it could be done, especially if it is hooked up to outside systems.

We believe that is a low risk in our system because they are not hooked up to outside systems.

Mr. DICKS. Is there encryption?

Mr. TODD. Yes, there is.

Mr. DICKS. Let us say a terrorist got control of the dam. Is there a way to override this system at the dam?

Mr. TODD. Yes, there is. We have operators on 24 hours a day. When we notice that the particular facilities that are controlled are not operating in the way that we believe they should be, we have manual controls. We do send our maintenance people out to check those. Sometimes we take over in manual control and operate the system manually just because there may be a glitch or something.

So, yes, we do have ways to do that.

Mr. DICKS. Do you have a comment there at the end,

Mr. Paller?

Mr. PALLER. Yes, I have a small comment. There are two other ways to connect to these.

First of all, the word SCADA doesn't cover all the control systems. We had a fight about that this morning. SCADA is just the distributed system; sometimes the very big gates use other systems called digital control systems.

I don't know to what extent those gates are not controlled by SCADA, but controlled by digital control systems. If there is a digital control system, most of those have dial-up access for maintenance ports, and Bill knows a lot about this.

So this idea—SCADA is not connected, doesn't define the whole problem. I am not saying that what—

Mr. DICKS. You are saying there are other vulnerabilities?

Mr. PALLER. There are other ways of getting into those systems besides the Internet. There are other systems that control those gates besides SCADA systems. Sometimes they are called DCS, sometimes they are called RTUs; they have got other names.

Mr. DICKS. Could hackers get into those systems as well?

Mr. PALLER. The FBI has reported that they already have. It might not be true. I mean, the only data I have got is, the FBI has reported it has.

Mr. DICKS. Interesting point.

Mr. PALLER. No, listen, it wasn't—it wasn't attacked.

Mr. DICKS. Now, does the Bureau of Reclamation, do you have control over the Army Corps of Engineers dams?

Mr. TODD. No, sir, we do not.

Mr. DICKS. So they are completely separate?

Mr. TODD. Yes, they are.

Mr. DICKS. All the private dams are separate?

Mr. TODD. Yes, they are.

Mr. DICKS. Are you working to try to develop best practices in the industry?

Mr. TODD. Yes, we have, especially on the physical side. We work directly with the Corps of Engineers and TVA and Homeland Security on those systems, and we are fully engaged in that. One of the outcomes of the Government Coordinating Council is to work with the private side and to get information sharing and communications going, so we believe that is working well.

Mr. DICKS. Mr. Purdy, they beat up on you pretty good today. Let me ask you this.

We spent a couple billion dollars, several billion dollars at the Department of Defense trying to put in place encryption on all kinds of different defense systems.

Have you benefited from any of that? Does Homeland Security get briefed on information from Defense about what they did to secure their systems?

Mr. PURDY. Yes. We have a close working relationship with the Information Assurance office within the Department of Defense, as well as a similar entity within the National Security Agency. So we share in the benefits of the information that they have gleaned and share with us.

Mr. DICKS. Can you give us any examples of anything that is been achieved?

Mr. PURDY. Well, I can't mention—I don't recall.

Mr. DICKS. If this is classified—I don't want to get into classified information obviously.

Mr. PURDY. I can't recall specific encryption benefits, but in those kinds of techniques, things as simple as making sure you encrypt the data not only in transit, but at rest, and how to protect those databases from attack are some of the examples of things that we have learned from them.

Mr. DICKS. Any comments on this point from any of the other witnesses?

Mr. RUSH. Yes. We have actually—completely, independently, as an industry organization, the American Gas Association got together with a group of people and put together an open standard. Any company can build it, and it provides a very high level of protection, not military grade, and it is an open standard. It is ready.

We have two manufacturers who have begun producing prototypes. It is ready to go. We are not talking something theoretical.

Mr. DICKS. Are people ordering it? Are companies ordering it?

Mr. RUSH. At this point they are opening ordering them in small numbers, yes, they are. But they are only ordering them in evaluation kits, typically about five.

Until it works and people have tested it, people will be slow to adopt them. But, yes, they are adopting them.

Mr. DICKS. Thank you, Mr. Chairman.

Mr. LUNGREN. I think we have about 6 minutes to get over to the floor to vote on the first 15-minute vote.

I want to thank this panel. I think it has been very helpful, very instructive. We make requests that all or some of you come back at another time, because this subcommittee—I am sure my cochair shares this—desires to continue to look at this.

I thank you all for your valuable testimony and the members for their questions. The members of the committee may have some additional questions for the witnesses, and they may submit them to you in writing. I would hope that you would answer those in a timely fashion. The hearing record will be held open for 10 days.

Mr. LUNGREN. The committee stands adjourned.

[Whereupon, at 5:40 p.m., the subcommittee was adjourned.]

APPENDIX

DR. K.P. ANANTH RESPONSES TO HON. DANIEL E. LUNGREN, AND HON. DAVE G. REICHERT, LETTER DATED NOVEMBER 8, 2005

I. *The Threat: Probability/Impact of Attacks on SCADA Systems*

1. Based on available research, how likely is an attack on a SCADA system?

Based on a review of 120 incidents, the current likelihood of a severe attack is low; but if the rate of incidents follows what has been seen for the Internet in general, we forecast that the risk will rise to a significant level in the future. Documented case histories show that activity has increased significantly since 1988. Many of these incidents come from the Internet by way of opportunistic viruses, trojans, and worms, but a surprisingly large number are directed acts of sabotage. Additionally, it is likely that there are many attacks not being reported because many asset owners are reluctant to share or report their experience.

SCADA systems are currently at risk from attacks stemming from a broad spectrum of attackers ranging from common Internet threats to directed attacks by individuals. The likelihood that SCADA systems are attacked in a manner that results in severe consequences is dependent on the potential attacker's motivation, intent, and expertise. SCADA systems are vulnerable and can be exploited to result in a disruption in service if an attacker invests enough time to learn the system before they attack. To date, the majority of reported attacks against SCADA systems have been the result of general Internet propagating viruses and worms that were opportunistic in nature and not directed.

2. What cyber security failures and incidents have you seen with SCADA networks?

Incidents to date have exposed poor security processes and vulnerable technology implementations. The lack of general awareness as to how the technology can be exploited has resulted in vulnerable technology implementations and weak security practices.

In the past, incomplete security efforts and risky practices have allowed common Internet attacks to randomly bleed into SCADA environments. In one example, servers infected before shipping by the manufacturer were mounted directly onto a control system network.

Security incidents impacting SCADA/control systems have been documented in 11 sectors. The largest number of incidents has occurred in the petroleum, power and utilities, transportation, and chemical sectors, which combine for over 70% of the incidents observed. None of the documented incidents have resulted in a significant event that resulted in loss of life, major disruption of service, or economic impacts. The US-CERT Control Systems Security Center (CSSC) has issued a report describing the reported incidents. (US-CERT Control Systems Security Center, *Industrial Security Incidents,* June 9, 2005)

3. Based on all available research, how frequently are SCADA networks attacked?

There have been only a few reports of directed attempts to penetrate and compromise operational control systems. However, there is no way to know with a high degree of confidence how many attacks take place because there is currently no formal center to report cyber attacks on control systems. A single reporting center is operated by the British Columbia Institute of Technology (BCIT). But reporting to the BCIT incident reporting system is purely voluntary. The BCIT primarily represents North America (Canada and the United States) with several members from the UK and Australia. It is doubtful that the reporting to the BCIT represents more that 10% of the total number of events. The CSSC has also collected incidents from several other reporting sources. These sources have documented approximately 120 documented cases in the past 20 years with the majority (more than 70%) occurring

in the past 5 years. Therefore, a reasonable estimate of the number of attacks, resulting in some damage, is between 20 and 200 per year. General cyber security monitoring at the perimeters of organizations using power sector SCADA systems has shown a higher rate of system probes and cyber reconnaissance activity than organizations belonging to other sectors.

This estimate includes a wide range of possibilities because actual incident reporting is very low. The low percentage of incidents that get reported is due to several factors, including:

- Organizations often perceive risk in reporting security incidents
- Many organizations lack the technical skill sets to detect sophisticated intrusions or to forensically investigate such activity
- Security technology is not well-suited for SCADA environments and existing technology have few features that lend themselves to detect attack activity
- Lack of general awareness as to the vulnerability of SCADA systems often results in not enough attention or efforts to detect attack activity.

The most immediate need in the arena of incident tracking is a more effective way of reporting cyber attacks (all or at least successful) on control systems. This enhanced reporting system needs to be a joint effort between industry and government and needs to provide anonymity to the reporter.

Technology trends will continue to create more vulnerabilities, and provide greater opportunities for threat actors to access control system networks. More interconnectivity and communication among cyber systems will lead to increased opportunities for talented people to breach the security systems and maliciously manipulate information or control system functions. We also anticipate this interconnectivity and communication capability to increase in control systems, at least for the foreseeable future. While access to operator information and denial-of-service attacks may cost industry money or result in embarrassment, the manipulation of system functions using this information can have more far-reaching consequences.

4. Is it possible to devise an attack to disable or disrupt a SCADA network for an extended period of time? If so, what is being done to mitigate such attacks?

Based on current testing and the knowledge of only a small number of actual control system implementations, we believe that cyber attacks can be devised to potentially disrupt SCADA systems (electric sector control systems) for as long as five to seven days. However, this does not necessarily translate into a failure of the physical system or controlled process for the same time frame. It is possible for a sophisticated attack to poison databases and files over time that would require a system re-build and re-configuration before the control system would function normally. More research is needed to investigate if cyber attacks can cause significant failures in long lead time physical equipment, such as transformers and generators. Similar studies are also needed in other sectors such as water, transportation, and chemical plants to assess equipment impact and downtime.

Our cyber security researchers have demonstrated the ability to physically destroy many of the IT components used in the control of a SCADA system. The practice is commonly referred to by hackers as "bricking" a box. There are many ways to require that a SCADA system be rebuilt from the ground up. Additionally, if the attacker plants a program in the backup sets ahead of time, the system will just destroy itself again as soon as it is brought back online. The attacker can also plant programs in non-essential equipment such as card readers, and printers that are unlikely to be found. The result is long-term disruption of service.

Many of the physical devices are set to automatically shut off at preprogrammed points to protect the devices from overheating/overdriving/overworking. In some instances an attacker can reset those points and drive the hardware to failure. Rhythmically turning on and off a 480-volt motor can destroy it. Operating a valve hundreds of times a second can destroy it. Flow-cooled pumps will overheat and fail if the valve is closed while the pump is running. Many other scenarios are easy to find and exploit.

Based on our testing in a representative configuration (an electric sector EMS system) established in the test beds, it is possible to disrupt system operation through cyber attack. The duration of the disruption will depend to a large extent on the types of attacks executed, the specific owner/user's system configuration, backup capability, and response/recovery practices. Mitigation efforts to date have focused on identifying specific vulnerabilities by examining representative systems in the test beds and providing information to system vendors who then eliminate the vulnerabilities in their products. Work in the test beds is also helping to identify the best practices that can be implemented by both the vendors and the users in

making their systems less vulnerable. A significant effort is being made to enhance owner and vendor awareness of the methods for reducing vulnerabilities.

5. (Not assigned)

6. Electric power is important for nearly all the things that Americans do—from businesses to schools to government to many forms of recreation. Has your research shown that the SCADA systems that control our power generation and distribution are fully protected from attacks launched from the Internet? If not, what kind of damage do your researchers believe smart, well researched attacks could cause?

Although some SCADA systems that control power generation and transmission currently have some form of cyber protection, power sector SCADA systems are not "fully protected" from Internet-launched attacks. Research has shown that the majority of vendor solutions are vulnerable to a cyber-based attack coming from the Internet and through the surrounding corporate network that could result in a complete loss of system control. Those attacks were successfully demonstrated despite the use of common configuration practices and the use of available security technologies (IDS, Firewalls, etc). For obvious reasons the majority of this research has not been replicated in the field but INL has the ability to create very large scale control system and physical infrastructure simulations in both the electric and chemical processing sectors.

We have also seen evidence of SCADA systems being vulnerable to non-expert-based attacks. In fact, non-directed common and opportunistic threats, such as viruses and worms, have impacted SCADA systems. Considering a random threat such as a virus can impact a SCADA system, a well resourced and motivated threat actor could compromise a control network and cause significant disruption to power SCADA systems. The disruptions may or may not result in wide-spread power outages depending on how much the attacker learned once inside of the target's control system. Certainly, a directed attack can result in injected commands being passed through the SCADA system to breakers in the field possibly resulting in breakers taking lines out of service.

Assessments performed in the test beds show that typical control systems can be compromised from the Internet if the attacker has some understanding of the system. Much of that system information can be obtained by a patient study of open source information. A well-orchestrated attack could provide the attacker with the capability to take over the operator's function, potentially without the knowledge of the operator. While strongly influenced by system configuration and operating policies, there is the potential to cause damage to equipment through the manipulation of operating and safety limit set points.

7. (Not Assigned)

8. We've heard a lot about the impact of a terrorist attack on a control system. But as we saw during Katrina, natural disasters can cause devastating impacts to our control systems infrastructures too. What kind of impact would natural disaster have on control systems in California (earthquakes), Oregon (Tidal waves/Tsunamis), The Gulf Coast (Hurricanes), elsewhere?

Any event, whether manmade or natural, resulting in the destruction of physical equipment and the loss of supporting services like water, power, and communications can negatively impact SCADA systems. Anecdotal information and data emerging from hurricanes Katrina and Rita are showing that, for SCADA and other control systems (and other utility operations), the need to plan and prepare for an "all hazards approach," rather than more narrowly defined scenarios, is crucial.

We learned from Hurricane Katrina that the main impact to a control system from a natural disaster is the remote entities that the system connects with (e.g. customers, substations, transmission lines). After the August 29th landfall of Hurricane Katrina in Louisiana, 2.7 million customers were without power, 263 substations and 181 lines were not operating. As of September 22nd, less than 250,000 customers are without power and 19 substations and 25 lines remain out (data from the Office of Electricity Delivery and Energy Reliability U.S. Department of Energy, Hurricane Katrina Situation Report #42, September 23, 2005). The control centers themselves are normally less vulnerable than the remote devices that are being controlled and queried for status.

The ability for a control system to minimize impact from a natural disaster is directly related to the system owner's continuity of operations, disaster recovery planning, and overall preparedness to handle natural disasters as discussed in the US CERT website (US-CERT Informational Paper September 16, 2005, produced by the US CERT Control Systems Security Center, Hurricane Katrina Control System Assistance *http://www.us-cert.reading*__room/KatrinaCSA.pdf).

The control system is only as good as the data it can receive. With limited view and communications, the systems? components and the applications designed for automatic control cannot be used properly without subject mater experts making the decisions. In the case of Katrina, the restoration process was hampered by the other communications outages of telephone and wireless.

The National Infrastructure Simulation and Analysis Center (NISAC) provides advanced modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies, vulnerabilities, and complexities. It would be helpful to study lessons learned during Katrina on the effectiveness of the NISAC models.

II. ***The Public/Private Relationship in Developing a SCADA Solution***

1. I understand the National Labs are conducting extensive research into SCADA and Control Systems. What resources are you currently lacking? How are you coordinating these efforts with the private sector? What can the federal government do to provide more resources?

Needed Resources: INL recommends a 5-year funding profile that allows the development of long-term programs to support critical infrastructure sectors immediate and long-term complex SCADA challenges. The uncertainty of year-to-year funding and funding delays at the beginning of the fiscal year negatively impact our ability to provide sustained research to identify vulnerabilities and to develop solutions to fix vulnerabilities aligned with asset owner and vendor-driven timelines.

Sustained funding will allow us to successfully decrease risks to control systems by conducting ongoing tests to identify vulnerabilities and develop mitigations, raising awareness and helping organizations develop the right mind set to protect SCADA systems, gaining access to more credible incident information, conducting in depth research and testing to explore possible consequences and outcomes, and monitoring the cyber underground to gauge their knowledge of and interest in SCADA systems.

Private sector coordination efforts: INL is working directly with asset owners and vendors to evaluate their system vulnerabilities and implementing mitigation steps. These evaluations are protected using a nondisclosure basis.

INL is engaging national experts from industry, national labs, and academia in dialog to keep current on allied research and best practices and to share that knowledge with industry. In FY–05, we conducted nine regional workshops and participated in the Process Control Forum. These interactions directly impacted 280 asset owners.

Our industry outreach program includes training and awareness demonstrations of the means and effects of a cyber attack on control systems. These demonstrations and training activities are ongoing with positive feedback from industry and government participants. These include live demonstrations of attacks/effects on small scale representative control systems for chemical and electric system processes and cyber security—control systems training uses these tools and subject matter experts.

Additional federal government resources: Along with sustained 5-year funding, designate INL as a National Center of Excellence and User Center for SCADA, Cyber Security, and Critical Infrastructure Protection. The Center would be modeled after existing National User Facilities at other DOE National Labs, such as the High Temperature Materials Laboratory at Oak Ridge National Lab or the Light Source Facility at the Brookhaven National Laboratory). The Center designation would capitalize on INL SCADA test beds and full scale infrastructure assets, build on our proven track record with asset owners and vendors to identify and mitigate cyber vulnerabilities, and provide an independent, scientific organization that tests and validates the vulnerabilities and identifies solutions. The result is federal/private partnerships with high value to the critical infrastructure owners and their vendors.

With long-term dedicated funding, INL can move from the current research approach, which focuses testing on specific attacks as a method of raising vendor awareness, to conducting extensive assessments in a comprehensive fashion. We would develop consistent methodologies and system rating approaches that would apply across all vendors and develop quantitative measures to verify the return on investment of research dollars that directly impact industry and taxpayers. To that end we would devote research focus to develop a realistic threat assessment methodology and then apply it to create an open, industry-acknowledged threat model for contingency planning.

2. (Not assigned)

3. It has been widely reported that both industry and the federal government find it difficult to estimate the economic impact of a cyber security

attack. Has the lack of actual quantifiable damages made the private sector leery of investing in cyber security?

There has long been widespread agreement that the published estimates of cyber-attack costs have little credibility. In April 2004, the Congressional Research Service Report on *The Economic Impact of Cyber-Attacks* concluded "No one in the field is satisfied with our present ability to measure the costs and probabilities of cyber-attacks." But the report resulted in limited research to address the measurement need. The research programs most directly addressing the need for better assessments of cyber-attack consequences are the programs of the U.S. Cyber Consequences Unit, a small independent agency established by the DHS in August 2004. The first of the larger US–CCU reports will be available for limited circulation release in early February 2006.

The lack of economic consequence data and security metrics has led to a variety of concerns about the possibility of a successful attack and its associated economic impact. Currently, there is no consensus about the level of resources that should be devoted to control systems cyber security. Standards and associated business cases are being developed that will help industry better evaluate the risk to their systems. Even with this lack of documented cases of quantifiable damage, attacks occur. For example, recent malware attack (Zotob) on multiple sites of a large manufacturing company resulted in loss of production time.

These types of attacks increase asset owners' awareness that they too could be the target of a potentially crippling attack; thus, investments are being made in the private sector. These investments tend to be dependent on the extent of awareness of cyber intrusions and the liability posed by denied services or business losses faced by individual companies as well as customer impact. Critical infrastructure sectors, such as electric utilities, chemical companies, oil and gas companies, and banks and financial institutions, realize the potential impact of cyber threats but the investments and attention paid is not uniform across the sectors. Cyber security concerns resulting from easy electronic access to accounts in the Banking and Financial Sector are addressed *USA Today's* November 2, 2005 first page article, "Cyber crooks break into online accounts with ease". In the Electric Sector, the required connectivity with neighboring systems creates a weakest link problem for the overall network of interconnected SCADA systems. The larger or more progressive utilities will suffer from weaknesses presented by smaller, resource-constrained neighbors.

Several industry associations, such as the Chemical Information Data Exchange (CiDX), the Water Environment Research Foundation (WERF), and the American Association of Railroads, are promoting cyber security among their subscribers. The Department of Homeland Security Control Systems Security Center (CSSC) established an Industry Interest Group to discuss asset owner's perspective of cyber security. Members of this group reported that at the operations levels within their company's organization, cyber security is important. However, at the board of director's level, cyber security seems less important because they may not see any risk to bottom-line profits. The group also reported that awareness communication tools would be helpful in convincing their management to invest in SCADA security, even though the perceived risk may be low at this time.

The reason the National Cyber Security Division of the DHS established the US–CCU, with the support of the National Communications System and help from the DHS Private Sector Office, was that both corporate executives and government officials regularly reported they could not justify larger cyber security budgets without better information on the likelihood and costs of possible cyber-attacks.

4. (Not Assigned)

5. Can you tell us specifically how your research on SCADA has, to date, impacted the way SCADA systems in the field are secured, and what percentage of those systems have been impacted? If that's not a big number, what is stopping us from putting the results of your research into practice in the field?

A result of our assessment work in the test beds is the identification of best practices that can be used to mitigate vulnerabilities by taking advantage of the capabilities already existing in the SCADA systems. Examples include ensuring fully patched operating systems, improving password management practices, and implementing layered security defenses (firewalls, DMZs).

SCADA system vulnerabilities identified through assessments performed in the test beds have been communicated to the manufactures and users of those systems. In all cases, the vendors have taken quick action to incorporate system modifications to mitigate the identified vulnerabilities in their new systems, but only 5% of installed systems are new systems. Thus implementing enhancements in currently

installed systems requires that owners be made aware of the vulnerabilities within their systems and the mitigating methods that are available to them.

More than 230 user representatives from over 100 major electrical industry owners/users of SCADA systems have been made aware of typical vulnerabilities and methods for security enhancement. The percentage of the industry that is represented by 100 owners is difficult to answer, but in very general terms we can say that they control approximately 80% of the power on the grid. This communication has been achieved through presentations and discussions in numerous electrical industry user group meetings and conferences. In addition to electrical industry interactions, workshops, demonstrations, training, and presentations have been provided to audiences responsible for control systems used across the Nation's critical infrastructure. In aggregate, these various forums have been attended by more than 7500 people from vendor and user companies.

In addition to assessments, cyber security awareness workshops in nine regions involved 480 industry participants during FY–05 have made the industry more cognizant of the need to strengthen their SCADA systems. In FY–06, we will be providing asset owners additional tools to strengthen SCADA security through vulnerability assessments both in test beds and at participant selected facility locations. The value of the INL work, as perceived by a sample of industry/end users, has been previously stated (see INL's written testimony of October 18, 2005, to the same Subcommittees).

We do not have access to data that would quantify the extent to which system owners are implementing our recommendations into their administrative and hardware/software management policies. This is typically information that is held close by the asset owners for competitive advantage reasons. Because the deployment of new systems occurs rather slowly (estimated at 5% annually for the installed infrastructure) the users, working with their vendors, can also design and implement mitigations specific to their systems. Thus the information we provide can be used to upgrade and improve configuration and management of currently installed systems.

The reason for relatively slow system upgrades is the high cost and the lack of a strong business case (bottom line dollar impact) to justify both the expenditure for improvements and to justify requests for recovery through the rate base. A frequently raised issue is that if the requirements for security upgrades were mandated through regulation, the asset owners would have a stronger basis for requesting rate relief. However this brings with it the added burden of additional regulation to the industry and is therefore not strongly supported by industry.

6. What has the money we have already spent on SCADA research done to improve SCADA security in the field?

The work performed and supported by the Department of Energy National SCADA Test Bed (NSTB) in the Energy Sector and the Department of Homeland Security Control Systems Security Center (CSSC) Program on the other sectors, have improved security at critical infrastructure facility sites in significant ways:

- **Awareness:** As a part of the mission for both the NSTB and the CSSC, cyber security awareness has increased in industry and government. Information on potential threats, vulnerabilities, and mitigation of cyber attacks on control systems has been disseminated through workshops, outreach, and training events at conferences, user groups, and invited sessions. The increase in awareness of the potential for real and serious impact to facility operations have resulted in asset owners performing reassessments of their cyber security for control systems.
- **Assessment and Testing:** CSSC and NSTB are engaged in performing assessments of major control system SCADA vendors? current products to identify both vulnerabilities and mitigation. Some of the vendors have taken steps to eliminate the identified vulnerabilities and shared the information with their users. Working closely with the vendors and the user community, the CSSC and NSTB provide a path to rapidly identify and facilitate the use of this information to increase the protection from cyber attacks. The success of these relationships act as models to both the vendor and user communities to work with these DOE and DHS programs. Several site specific assessments have also been conducted at the request of asset owners. Results of these assessments provide direct and specific input to increasing SCADA security at those sites.
- **Technology Development:** A key element of the CSSC program is the identification and quantification of risk that supports a business case to the asset owner for the policy, time, and equipment investments to reduce risk to acceptable levels. The characterization of vulnerabilities (control and network systems), consequences (safety and national security), and threats (beginner level

to hostile nation state) coupled with the cost of implementation of safeguards is a necessary step in developing risk models and the business case. The CSSC is active in working and coordinating efforts with industries, industry and trade associations, government agencies, and academia to identify gaps in technologies and standards to apply to both current and legacy critical infrastructure control systems. While these efforts are emerging, the broad exposure of this work and participation of the stakeholders will produce improvements in SCADA security that meet the need for information protection coupled with business constraints and will increase security awareness.

• **US–CERT Support:** The United States Computer Emergency Response Team (US–CERT) provides response and capabilities to support government and the private sector dealing with cyber threat and attacks to the Nation's network communications and computing infrastructure. The CSSC augments this capability by providing expertise in control systems and the potential vulnerabilities and impacts of cyber attacks. The CSSC has a broad reach of assets within the national laboratories and private sector to assess situational awareness during specific response to events reported to the US–CERT. The CSSC, as a part of the US–CERT in these activities, can issue alerts to be distributed at a national level given that their may be real and significant threats to control systems for certain sectors or user communities. The goal of this capability is to provide another level of information to those asset owners to increase SCADA security to threats.

7. Is there any risk of duplicating efforts with the lab beds at Sandia and Idaho and other research around the country?

INL is directly involved in two programs, the National SCADA Test Bed sponsored by DOE/OE for the Energy Sector and the CSSC Program sponsored by DHS/NCSD for the other sectors. We are working with Sandia and others to complement what is needed to carry out the objectives of these programs and there is no duplication of efforts. Also to prevent the duplication of efforts, the sponsors (DOE/OE and DHS/NCSD) review the scope of work on the NSTB and Control Systems Security Center Programs.

INL and Sandia each have unique and complementary SCADA capabilities. INL focuses on evaluating Cyber Security vulnerabilities of SCADA systems deployed in operational facilities and validating solutions; and penetration testing of control systems. Also INL has on-site, full scale infrastructure systems such as electric transmission systems, substations, a pilot chemical plant and communications test beds that enable field scale evaluations. Sandia, on the other hand, has information technology red teaming and assessment capability, cryptography, and bench scale testing capability complementing INL's capabilities. The two Labs recognize their strengths and collaborate to provide the service needed to support asset owners and vendors.

Because of the number and diversity of infrastructure facilities in the US requiring SCADA/Cyber security and the level of coordination of efforts between INL and Sandia, there is great value in having two national labs with capability and capacity to provide a wide range of assessment services to asset owners.

INL, as the lead lab for the control system cyber security program coordinates efforts between labs utilizing specific expertise, facilities, and capabilities at each laboratory to perform its work. In January of 2005, a Leadership Steering Group was organized and consists of members from Idaho National Lab (INL), Sandia National Lab (SNL), Pacific Northwest National Lab PNNL), and Lawrence-Livermore National Lab (LLNL). The Group meets on a quarterly basis to discuss the direction of the program, coordinate efforts and deliverables, and identify expertise that is needed to solve issues and challenges. Ideas are exchanged and security products developed for various governmental customers are shared.

III. ***The Federal Government's Role in Cyber Security***

1. (Not Assigned)
2. (Not Assigned)
3. (Not Assigned)
4. (Not Assigned)

5. There are several SCADA test beds across the country. Is there any risk of duplicating efforts with the lab beds at Sandia and Idaho and other research? Is there anyway to consolidate these efforts?

INL is directly involved in two programs, the National SCADA Test Bed sponsored by DOE/OE for the Energy Sector and the CSSC Program sponsored by DHS/NCSD for the other sectors. We are working with Sandia and others to complement what is needed to carry out the objectives of these programs and there is no duplica-

tion of efforts. Also to prevent the duplication of efforts, the sponsors (DOE/OE and DHS/NCSD) review the scope of work on the NSTB and Control Systems Security Center Programs.

INL and Sandia each have unique and complementary SCADA capabilities. INL focuses on evaluating Cyber Security vulnerabilities of SCADA systems deployed in operational facilities and validating solutions; and penetration testing of control systems. Also INL has on-site, full scale infrastructure systems such as electric transmission systems, substations, a pilot chemical plant and communications test beds that enable field scale evaluations. Sandia, on the other hand, has information technology red teaming and assessment capability, cryptography, and bench scale testing capability complementing INL's capabilities. The two Labs recognize their strengths and collaborate to provide the service needed to support asset owners and vendors.

Because of the number and diversity of infrastructure facilities in the US requiring SCADA/Cyber security and the level of coordination of efforts between INL and Sandia, there is great value in having two national labs with capability and capacity to provide a wide range of assessment services to asset owners.

INL, as the lead lab for the control system cyber security program coordinates efforts between labs utilizing specific expertise, facilities, and capabilities at each laboratory to perform its work. In January of 2005, a Leadership Steering Group was organized and consists of members from Idaho National Lab (INL), Sandia National Lab (SNL), Pacific Northwest National Lab PNNL), and Lawrence-Livermore National Lab (LLNL). The Group meets on a quarterly basis to discuss the direction of the program, coordinate efforts and deliverables, and identify expertise that is needed to solve issues and challenges. Ideas are exchanged and security products developed for various governmental customers are shared.

6. (Not Assigned)

IV. *The Federal Role in the Future*

1. Based on your knowledge of the SCADA research field, what are the most promising technological breakthroughs you see that can protect our SCADA systems in the short term? I realize there are no silver bullets, but please list the solutions that will actually work to protect our SCADA systems.

Various emerging technologies show promise in protecting control systems. Deep packet inspection engines (optimized to detect control system packets) can guard for commands or injects traveling through unauthorized avenues like the organization's perimeter or corporate network. Memory cache integrity technologies can be used to detect malicious events like buffer overflows. Secure authentication approaches applied to SCADA protocols and emerging low-overhead encryption techniques are also promising. The optimization and use of these emerging security technologies should reduce some of the risk SCADA systems now face. In order to bring these technologies to bear more testing environments need to be used to test general IT security solutions and enhance them to work in control system environments.

Near-term security enhancements can be most effectively implemented through taking advantage of existing technologies. This can be done through the definition and implementation of security policies based on the best practices identified in the test bed efforts and in industry. Best practices include defining the electronic perimeter, setting up layered defenses, monitoring communication traffic for anomalies (such as with intrusion detection and prevention devices), and establishing strong password management and system patching policies. Encryption technologies should be applied to eliminate plain text communication that can be monitored by an intruder to obtain system knowledge.

On a longer term basis, secure programming techniques should be used in application code development as is now being done for operating systems and embedded applications.

Much knowledge exists, but there is a gap between general IT security and SCADA security. SCADA systems have to be ultra-reliable and ultra-stable. If cybersecurity is going to take hold in SCADA networks, the following must take place: (1) a testing location where a utility can test their configurations with expert support and advice must be developed and (2) a user community where users of the same SCADA system with the same problems can critique their architectures and perform peer reviews must evolve.

2. How do we make rapid progress in improving security in the field?

Increasing awareness among asset owners and vendors should be a priority because vendors must eventually implement the security measures. Another priority should be providing the ability to test the systems in an impartial manner. Third

is providing the tools that are needed to mitigate the vulnerabilities and secure the systems. Finally, some consideration is required for financial incentives to accelerate cyber security implementation by asset owners. In all of these steps we should also look at the interlinked aspects of information technology, control systems and telecommunication and take a systems approach to dealing with this challenge. The key to success lies with increasing industry awareness, and industry associations can play a critical role. Many of these groups have already seen the need for improving cyber security in control systems and have started working groups or sub-committees to address the issues and share information with their subscribers. As NCSD shares vulnerability findings and provides best-practices for mitigation to these associations, they are transmitted to their members and mitigations are implemented.

A good example of the security initiative within industry is the Chemical Information Data Exchange (CiDX). In January 2003, CiDX started the Chemical Sector Cyber Security Program. This program has a sub-committee that is devoted specifically to cyber security for control systems. They recently recommended that the CiDX subscribing companies perform self-assessments of their control system security posture. Several companies reported results at the October CiDX General Membership meeting in Houston. While, these self-assessments are still immature, their willingness to improve their security posture is commendable. The NCSD has developed a self-assessment tool to help associations like CiDX improve the effectiveness of their self-assessment process. The tool will assist asset owners to focus on the critical cyber security requirements and associated compliance strategies to achieve improvements in security. In FY–06, the self-assessment tool will be piloted with several asset owners in multiple sectors. After the piloting effort, NCSD will improve the tool, provide training at workshops in the various associations, and commence wide-spread distribution and use of the self-assessment tool. This will give asset owners specific measures for immediate implementation and reduction cyber security risk.

Rapid progress is based upon a multi-tiered approached that involves diverse stakeholders. This includes system integrators, vendors, and asset owners. Increasing security in the field will require each one of these stakeholders to develop better integration requirements that include improved security, hardened vendor systems, and increased situational awareness, respectively. Asset owners need to increase their awareness to control system cyber security and the inherent reliability benefits to addressing security, thereby requesting that secure system be purchased and integrated into the field.

3. (a) Has the federal government advocated for standards establishing a minimum floor for securing control systems?

While the argument could be made for a minimum floor standard, this may not be the solution for the long term. Since 85% of our critical infrastructure is owned by the private sector, it is their responsibility to adequately protect their assets and deliver the services and products to the customer at large. The liability that could result from a federally mandated minimum standard argues against such a standard. Also, the need for continuous improvement is disincentivized by a minimum standard. In our view, industry groups working together should come up with the best practice for their industry segments. The electric utility, chemical industry, and oil and gas industry have all come up with some type of best practice and they should be encouraged to make more widespread use of these practices. Similarly, other industries should come up with best practices for their segments with help from the federal government in terms of testing vulnerabilities and developing mitigation measures.

The DHS (CSSC Program) and DOE (NSTB Program) both include tasks to support improvements to industry security standards. In addition to an ongoing review of standards applicable to control system security (with the goal of identifying areas that should be strengthened), activities include support to drafting ISA's SP–99 and a technical review and assessment of the standard for Secure ICCP.

3. (b) What would a minimum floor look like?

A minimum baseline standard should address areas that are important to cyber security in general, with an additional emphasis on areas that are of particular concern to control system security. Control systems are complicated and varied depending on their application. Developing standards that address security needs has begun (as outlined below, Question 3-e) but addressing the hundreds of needs for securing the complexities of control systems will require a large concentrated effort.

Topics that should be addressed include: the assessment of risk, development of a security policy, organization of information security, management of assets, human resources, physical and environmental security, management of operations, access control, the acquisition, development, and maintenance of process and infor-

mation systems, incident and business continuity management, compliance with legal and company policies. Standards should also address next generation systems to help ensure that security in "built into" emerging components and systems.

Another area of concern is system integrators. Standards must also address network architecture to ensure that security vulnerabilities are eliminated at the system level.

The CSSC has developed a cyber security protection framework that includes hundreds of high-level security requirements for the various components and communication links in control systems. These requirements have been compared with the myriad of existing cyber standards to identify gaps and overlaps in these standards. In FY–06, the findings of this review, along with continued reviews, will be used to recommend specific changes and improvements to the various standards bodies.

3. (c) Have industries leaders begun the process of developing those standards already?

Several industries, particularly chemical, oil and gas, and electrical, have made great strides in the development of control system cyber security standards. In addition, professional organizations and government bodies have contributed to the development of these standards.

3. (d) Has the government established any "best practices" that can be modeled by industry?

As mentioned above (Question 3–b), CSSC has collected an initial set of industry best-practices for complying with security requirements and standards. NSTB program is developing best practices aimed at mitigating the common vulnerabilities discovered during control system testing.

Through both NSTB and CSSC Programs, best practices are being identified and shared with industry as stated in II–5.

3. (e) What other standards activities are being developed besides AGA 12?

Several cyber security standards aimed at industrial control systems have been developed or are in the process of development. Some of these may not be considered as standards in the strictest sense, but still provide guidance and direction. These include:

AGA 12—The American Gas Association is in the process of developing a series of four standards recommending practices designed to protect SCADA communications against cyber attacks. To date, Parts 1 and 2, which address Cryptographic Protection of SCADA Communications, are still in draft form.

API 1164—The American Petroleum Institute released this standard on SCADA security to provide guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. This document was released in September 2004.

CIDX—The Chemical Industry Data Exchange has developed a *Guidance for Addressing Cybersecurity in the Chemical Sector Version 2.1.* This document describes key elements of a cybersecurity management system in the chemical sector.

IEC 62351—The International Electrotechnical Commission is in the process of developing "Data and Communication Security."

ISA TR 99 Parts 1 and 2—The Instrumentation, Systems and Automation Society (ISA) has published two technical reports addressing control system security with suggestions for securing control systems against cyber attack.

ISA SP99 Parts 1 and 2—ISA is in the process of developing two control system cyber security standards. These standards, still in draft form, will provide requirements for securing control systems.

NIST SPP–ICS—NIST has developed and released a System Protection Profile (SPP) to formally state security requirements associated with industrial control systems (ICS).

NIST 800–82—NIST has developed SP800–82, a Guide for SCADA and ICS Security. It is in draft form with scheduled release January 2006.

NERC 1200—The North American Electric Reliability Council (NERC) has developed and released this temporary standard to establish a set of defined security requirements related to the energy industry and to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.

NERC CIP–002 through—009—NERC is in the process of developing a series of standards aimed at entities performing various electric system functions. When released, it will replace NERC 1200.

4. (Not Assigned)
5. (Not Assigned)
6. (Not Assigned)

7. Some have mentioned the value of a "vendor" incentives system that would provide tax and other financial incentives to manufacturers who are producing control systems that are already in "best practices" compliance. How feasible is this, and have there been evaluations of the cost to the federal government?

The first step in incentivization is enabling full reporting and disclosure of cyber security incidents, without attribution, similar to the FAA's Airline Pilot Reporting System. Included in this Cyber Security Reporting should be disclosure of the stringency level and thoroughness level of the reporting and assessments, so the frequency and magnitude of the problems can be analyzed. Then appropriate mitigation steps and incentives for implementation of these steps could be developed. With this incident information, other incentive options could be considered in light of the overall risk/benefit ratio.

Another incentive would be to enable independent third-party testing and evaluation of control systems and techniques to mitigate vulnerabilities as is now provided through the DOE/NSTB Program to utilities and through the DHS/CSSC Program to all other industry sectors.

The feasibility and cost of incentives would need to be studied closely to ensure the approach provided the right reward to maximize responsible action by vendors. The best vehicle, approach and resulting cost to implement have not been studied.

8. (Not Assigned)

V. *Dam Security*

(None Assigned)

DONALD ANDY" PURDY RESPONSES TO THE HONORABLE BENNIE G. THOMPSON QUESTIONS

THE THREAT: PROBABILITY/IMPACT OF ATTACKS ON SCADA SYSTEMS

• Based on all available research, how likely is an attack on a SCADA system?

Response: Attacks are already occurring against Supervisory Control and Data Acquisition (SCADA) systems/control systems; however, the number of incidents reported is few and the consequences associated with these reported attacks are generally not very significant. The NCSD Control System Security Program (CSSP) has reviewed data on approximately 120 documented cyber incidents against SCADA/control systems over the last 20 years. This data shows that the number of cyber attacks reported against SCADA/control systems has been increasing over the last several years and also shows that a larger percentage of attacks are coming from external sources as opposed to internal sources.

As SCADA/control systems have greater interconnectivity to information technology (IT) systems external to the SCADA/control systems operating environment and increase their utilization of common open standards and protocols, the exposure of systems to outside entities and the number of vulnerabilities present in the control system environment will continue to increase.

Insufficient data currently exists to accurately calculate the likelihood of a successful cyber attack against a SCADA/control system that would result in a catastrophic consequence. However, based on current scenarios developed by industry and the National Labs, the National Cyber Security Division (NCSD) believes that as the number of vulnerabilities, the number of people with intent to cause the U.S. harm, and the number of people with sufficient skills and capability to successfully execute an attack continue to increase, the likelihood of a successful cyber attack of significant consequence against SCADA/control systems will continue to rise. The NCSD CSSP is working under the assumption that a cyber attack resulting in a significant consequence is likely to occur some time in the future. We are aggressively pursuing mitigation remedies to reduce the likelihood of cyber attacks on SCADA/control systems.

NCSD is establishing a control system cyber attack response center through the United States Computer Emergency Readiness Team (US-CERT) with technical response teams active within the CSSP. The Cyber Storm exercise beginning in February 2006 will provide additional information on readiness and response capabilities and needs.

NCSD is also working with the Intelligence Community to better collaborate on SCADA/control systems threat requirements and provide input on intelligence products.

• **Based on all available research, how frequently are SCADA networks attacked?**

Response: Historically, there has been no consensus on a formal center in the U.S. for all critical infrastructure owners and operators to report cyber attacks against SCADA/control systems. US-CERT recently initiated efforts to serve as the central focal point for the nation's critical infrastructures to report SCADA/control systems cyber incidents and vulnerabilities.

A reporting center operated by the British Columbia Institute of Technology (BCIT) also accepts voluntary submissions of SCADA/control system incidents. Owners and operators of U.S. critical infrastructures are hesitant to report SCADA/control system cyber incidents both because of concerns about how the information could potentially be used to harm the reporting organization, and also due to the absence of a clearly designated place to report cyber incidents.

The NCSD CSSP combined cyber incident information from BCIT with information from other sources to examine approximately 120 documented cases occurring over the past 20 years. A majority of these reported SCADA/control system incidents (>70%) have occurred in the past 5 years. However, it is widely viewed that the number of incidents are highly underreported. We are working with SCADA/control system vendors, owners and operators to raise awareness and increase cyber incident reporting to the US–CERT.

• I am interested in your assessment of the type of damage that you believe can actually result from a terrorist attack on SCADA systems. I think many people were shocked when on September 11, 2001, they learned that a single airplane could cause one of the World Trade Towers to collapse with huge loss of life. **What are the corresponding scenarios for catastrophic damage that can be caused by someone who has taken the time to learn to control SCADA systems?**

Response: Intermittent or properly timed loss of control of a critical infrastructure control system can enhance the probability of incorrect operator responses, which can lead to accidents with serious physical results, such as fire, explosion, collisions, or loss of production.

Two historic events affecting critical infrastructures where control systems could have played a contributing role include explosions at the Piper Alpha North Sea Platform and the Texas City oil refinery. The Piper Alpha platform explosion in July 1988 killed 167 and resulted in losses which are estimated up to $15.2 Billion US. Although there was a combination of events that lead to this accident, incorrectly interpreted signals and early loss of the control room contributed to the disaster. The March 23, 2005 Texas City oil refinery explosion killed 15 and injured 170, and cost close to $1 Billion US. This accident did not involve a cyber attack, but the accident evolved as a result of the misinterpretation of signals and indicators, which could be affected by a cyber attack.

The following are some examples of scenarios that show how cyber intrusions could result in physical damage, loss of life, environmental damage, economic loss, and/or loss of production in our nation's critical infrastructures.

—The breach of security controls in the transmission mechanism for a regional power grid system could potentially allow a strategic attack to develop into a widespread blackout due to the unique cascading aspects of power transmission. Although the August 2003 East Coast blackout was not caused by a cyber attack, the failure mechanisms that caused that blackout are similar to those that could be achieved through a cyber attack.

—The readings on chemical mixing tanks during the batch process could be tampered with by unauthorized network intrusion, forcing lethal and highly combustible reactions to occur without warning to the operators. Misinformation, exacerbated by improper response, is the cause of many industrial accidents.

—Rogue access into the railway switching system within a major city could cause significant gridlock to commuter traffic and import/export functions or potentially result in a train collision.

—In a blended physical and cyber attack, quality and safety triggers in a metropolitan water facility could be subtly compromised allowing for normally unallowable levels of toxins or chlorine to be distributed into the city reservoirs and pumping systems.

—According to the Network Reliability and Interoperability Council (NRIC),[1] the growing use of Voice Over Internet Protocol (VOIP) and the interconnected nature

[1] The Network Reliability and Interoperability Council (NRIC) is a partnership of private sector entities and the Federal Communications Commission (FCC) that develops recommendations designed, in part, to assure optimal reliability, security and sustainability of the nation's telecommunications infrastructure during periods of exceptional stress, including terrorist attacks or similar occurrences. http://www.nric.org/

of networks pose an increasing risk to the telecommunications infrastructure, in part because internet-based protocols are not as robust against security breaches as is traditional telephone technology. If operations centers or network management functions are compromised by combinations of cyber and physical attacks there could be a cascading effect that disrupts the communications capabilities of consumers, businesses and emergency first responders.

THE FEDERAL GOVERNMENT'S ROLE IN CYBER SECURITY

• We saw during Hurricane Katrina that the federal government is unprepared to respond to a large natural disaster. Today we've heard about the devastation that may be caused if a terrorist or a natural disaster hits our control systems. Just last week, a headline in the New York Times read: "US cyber security due for FEMA-like calamity?" **Are we prepared for a cyber attack on our control systems? Similarly, if a natural disaster hits our control systems, are we prepared to respond to that?**

Response: The NCSD CSSP is being proactive in preparing for events, both natural and man-made, that could potentially disrupt our nation's control systems and the critical processes and functions they monitor and manage.

A major initiative being pursued by NCSD CSSP to prepare for catastrophic events against our nation's control systems is the on-going effort to expand the US–CERT's current capability for responding to cyber incidents and vulnerabilities to include the ability to respond to incidents involving control systems. The NCSD CSSP provides the US–CERT Operations Center with control system expertise and support in responding to control system related incidents and in managing vulnerabilities affecting our nation's critical control systems. An important component of this US–CERT control system support is the utilization of the knowledge, resources, and control system expertise and cyber security expertise available among the national laboratories and the control systems community.

NCSD is creating the infrastructure and processes to specifically deal with both cyber attacks against control systems and also natural disasters that affect control systems. NCSD received positive feedback from the control system community in response to the informational focus paper the US-CERT released to the control system community to assist owners and operators in restarting their control systems safely and securely in response to Hurricane Katrina. This document is available on the US–CERT web site: ***http://www.us-cert.gov/reading—room/KatrinaCSA.pdf.***

• On August 12, committee staff was told in a briefing with DHS officials that there are only two full-time DHS employees working on control system issues. **How many DHS employees are currently working on SCADA/control system issues?**

Response: NCSD has authorized three government full time equivalent (FTE) billets for the CSSP. Currently, two of those three positions are filled and the third is expected to be filled in Q2 of FY06. In FY04, NCSD's CSSP determined that the control systems expertise necessary for the program to perform its mission was not readily available within the government and sufficient authorized FTE billets were not available at that time. In FY04, the CSSP conducted research to identify programs, facilities, capabilities, and resources, including national laboratories, which possess control systems and associated cyber security expertise and resources. NCSD utilizes these identified resources and capabilities to achieve mission goals and objectives.

• The Department established the Process Control System Forum (PCSF) to facilitate communication between government, industry, vendors, and academia. **How effective has this endeavor been? How frequent have the meetings been?**

Response: The PCSF is a relatively new endeavor and it is difficult to assess its effectiveness at this point in time. DHS plans to conduct an independent audit of the effectiveness of the PCSF in Q3–FY06. The value of the PSCF is its ability to reach out to representatives from all of these stakeholder groups in all critical infrastructure sectors (such as chemical, water, energy and others) that utilize and rely on SCADA/control systems. The PCSF met four times in FY05 with its next meeting scheduled for June 6–7, 2006 in La Jolla, California

• DHS has gone through four cyber security managers—Richard Clarke, Howard Schmidt, Amit Yoran, and Robert Liscouski. **How has turnover on the DHS cyber security team impacted the effectiveness of DHS to deal with a cyber attack? Mr. Liscouski left in January—Why hasn?t Secretary Chertoff appointed a replacement?**

Response: Addressing organizational issues is central to Secretary Chertoff's "Second Stage Review" (2SR) of the Department. The 2SR details a six-point agenda that includes improving DHS financial management, human resource development,

procurement, and information technology, and realigning the DHS organization to maximize mission performance. Recognizing the importance of protecting critical cyber assets, Secretary Chertoff is increasing the authority for cyber security by placing the coordinated activities of the NCSD and National Communications System (NCS) under an Assistant Secretary for Cyber Security and Telecommunications. The new Assistant Secretary will report to the new Under Secretary of Preparedness. We expect that the new Assistant Secretary will be named in the near future.

• There are several SCADA test beds across the country. **Is there any risk of duplicating efforts with the lab beds at Sandia and Idaho and other research? Is there any way to consolidate these efforts?**

Response: The NCSD CSSP completed an evaluation that identifies control system security-related programs among national laboratories, academic institutions, and agencies. This initiative evaluated the respective value of other's work to the CSSP; and provided recommendations on how selected program activities could be leveraged to reduce control system vulnerabilities. The focus was on domestic public sector programs because they could be more readily leveraged than activities in the private and international sectors. The results of this evaluation were utilized to identify where duplication of efforts might exist and also served as a roadmap to identify which groups the CSSP should work with.

The Department of Energy's Idaho National Laboratory (INL) has been designated as the lead national laboratory in supporting the CSSP. However, the CSSP funds initiatives with several DOE national laboratories and the control systems community through a contract with INL. INL has been assigned the role of coordinating and leveraging efforts between labs utilizing specific expertise, facilities, and capabilities at each laboratory to perform its work. In January 2005, a Leadership Steering Group was organized, which consists of members from INL, Sandia National Lab, Pacific Northwest National Lab, and Lawrence-Livermore National Lab. The Group meets on a quarterly basis to discuss the direction of the program, coordinate efforts and deliverables, and identify expertise that is needed to solve issues and challenges. Ideas are exchanged and security products that are developed for various governmental customers are shared.

Moreover, utilizing more than one lab allows for additional development and verification of efforts. If only one group is able to address an issue, then the best achievable results are limited to what that group develops. Competition is a motivating force that compels people to work harder and faster to produce the greatest advances and best solutions. Constructive competition exists among those who are attacking SCADA/control systems, and therefore it is important to encourage competition among those seeking to protect our systems.

• This is more of a general question about fundamental Internet protocols. There has been significant discussion in the technology world about the security of the basic, underlying Internet protocols. **In your opinion, how secure are these protocols? Is this something that DHS is examining?**

Response: There are, and likely will continue to be, security issues with Internet protocols. The Internet Engineering Task Force has a Security Area, *http://www.ietf.org/html.charters/wg-dir.html#Security%20Area,* which has a number of individual working groups addressing these issues. NCSD currently does not have any efforts or projects dedicated specifically to studying a particular protocol, although efforts are underway within DHS to model SCADA/control systems to better understand the disruptive effects of internet congestion to SCADA/control systems and the effectiveness of Next Generation Priority Services (NGPS) against these disruptions.

There is a significant challenge with the lack of security, or verifiable security, in core internet protocols. Some application level protocols (such as Secure Shell and Secure Socket Layer) and their implementations have improved their security over the last few years. However, the core security problems with underlying protocols, transport layer and below (e.g., Transmission Control Protocol/Internet Protocol and Address Resolution Protocol), create long term security problems. Although some credible attempts at improving these underlying protocols are ongoing (e.g., Internet Protocol Version 6), the question of their overall security remains unanswered.

The National Strategy to Secure Cyberspace (NSSC) calls out the fact that there are challenges with the existing Internet infrastructure. As a step toward fulfilling its responsibility for coordinating implementation of the NSSC with respect to the domain name system (DNS) infrastructure, DHS S&T is working to deploy the DNS Security Extensions (DNSSEC) protocol. The DNSSEC effort will enhance the security of a fundamental element of the Internet infrastructure. DNS is the hierarchical naming system that maps IP (Internet Protocol) addresses to more user-friendly but structured names; the extensions to the original protocol consist of a hierarchy of

cryptographic signatures that assure the integrity of the DNS queries by providing origin authentication of DNS data, data integrity and authenticated denial of existence. These measures protect against tampering in caches and transmission and enhance the infrastructure's security, thus contributing to increased trust in the Internet and systems, services and markets that rely upon its secure operation. The DNSSEC protocol has been under development for more than10 years and was approved by the IESG in October 2004; it is awaiting final publication. The goal of this effort is to enable all DNS traffic on the Internet to be DNSSEC compliant. In operational terms, this goal translates into the following ideal: Every lookup request requires and receives only DNSSEC-validated answers. Achieving this operational goal occurs within the framework of four principal and interrelated tracks: technical, organizational, education and outreach, and public policy. The primary focus of this effort is on the technical issues and process of adoption and the organizational and outreach/ educational activities required to achieve resolution of the technical objectives and activities. DHS S&T has been responsible for coordination among government agencies, namely Department of Commerce (DOC), Office of Management and Budget (OMB), General Services Administration (GSA), Department of Defense (DOD), and several others.

The NSSC also calls out the fact that there are challenges with the existing Internet routing infrastructure. As a step toward fulfilling its responsibility for coordinating implementation of the NSSC with respect to the routing infrastructure, DHS S&T is working with government and industry through the Secure Protocols for the Routing Infrastructure (SPRI) program within the S&T Directorate. DHS S&T has organized a series of workshops in the SPRI program to formulate an approach and a roadmap for securing the Border Gateway Protocol (BGP) in the Internet routing infrastructure. This workshop series has brought together people from academia, research institutions, government, and industry who have a thorough understanding of BGP technology, of BGP use in the Internet today, and of the business of providing internet service. Several techniques to secure BGP have been suggested, but none has won acceptance in terms of completeness, scalability or deployability. The workshops have been working towards a consensus of an acceptable, deployable security technique and a strategy for deployment. The SPRI initiative has been successful at bringing together the major Internet Service Providers (ISPs), router vendors, large-scale end users, government, and academia to identify a path forward to harden the routing structure of the Internet. This has included working with the major Internet registries, such as the American Registry of Internet Numbers (ARIN) and Reseaux IP Europeens (RIPE), and international participants from forward-looking countries, such as Sweden, Netherlands, and Japan.

Relative to control systems, this issue is important because many companies are now using standard Internet protocols to communicate between the control room and the enterprise network. Control systems vendors are beginning to use core Internet protocols as their bottom-most communication mechanisms on control system local area networks. Control system specific protocols tend to be insecure because they were not designed with security as a dominant focus, many are proprietary and depend on "security through obscurity," and control system protocols have generally not been exposed and stressed from a large number of concentrated attacks from hacker groups.

• In 2003, the President, as part of an initiative to protect American infrastructure, ordered the Department of Homeland Security to create The National Infrastructure Protection Plan. This plan was due in December 2004. DHS released an Interim Report in February, 2005, which was criticized by the GAO for being incomplete. At the time the Interim Report was created, DHS pushed the due date for the Final NIPP back to November, 2005. *When will the Office of Infrastructure Protection finalize the NIPP? What is the role of the National Cyber Security Division (NCSD) in NIPP? What role will your office be playing in the "Final NIPP"?*

Response: The draft NIPP Base Plan was released for final review and comment on November 2nd, and addresses the Federal, State, territorial, tribal, local, and private sector roles and responsibilities for critical infrastructure protection. It will be completed in early 2006. The 17 critical infrastructure and key resource (CI/KR) Sector-Specific Plans (SSPs) will further detail risk reduction strategies related to their respective critical cyber infrastructure.

As part of NCSD's participation in the development of the National Infrastructure Protection Plan (NIPP), NCSD is ensuring that the NIPP Base Plan includes content to address cyber security and the cross-sector/cross-border cyber element of CI/KR protection across all 17 sectors. NCSD also highlights cyber security concerns in an appendix to the Base Plan that provides additional details on processes, procedures, and mechanisms needed to achieve NIPP goals and the supporting objectives for cyber security. The cyber security appendix specifies cyber responsibilities for se-

curity partners, processes and initiatives to reduce cyber risk, and milestones to measure progress on enhancing the Nation's protection of cyber infrastructure.

After the release of the "Final NIPP," NCSD will continue to work with the relevant stakeholders to address cyber security and the cross-sector cyber element of CI/KR protection as outlined in the draft. This will include developing the Information Technology Sector Specific Plan as the designated Sector Specific Agency for the IT Sector, providing guidance to other Sector Specific Agencies to address cyber security, and coordinating international aspects of cyber infrastructure protection.

• According to a New York Times article last week, DHS is spending $17 million of its $1.3 billion science and technology budget on cyber security. Committee staff was told in a briefing with DHS officials that there are only two full-time DHS employees working on control systems issues. *Do you think the Department is devoting enough attention and resources for cyber security?*

Response: The Department is devoting significant resources and attention to the important area of cyber security, as described in the detailed answers to the questions above. NCSD and S&T continue to partner effectively to produce tangible results in an area that is constantly evolving. As described above, the NIPP provides a framework and roadmap for progress and unites Federal, State, local, and tribal governments and the private sector in the process for studying and identifying solutions to mitigate cyber risk. Additionally, recognizing the importance of protecting critical cyber assets, Secretary Chertoff is increasing the authority for cyber security by placing the coordinated activities of the NCSD and NCS under an Assistant Secretary for Cyber Security and Telecommunications. The new Assistant Secretary will report to the new Under Secretary of Preparedness. We expect that the new Assistant Secretary will be named in the near future.

QUESTIONS FOR THE RECORD FROM THE HONORABLE BENNIE G. THOMPSON FOR LARRY TODD

TOPIC I. THE THREAT: PROBABILITY/IMPACT OF ATTACKS ON SCADA SYSTEMS

Question: Based on all available research, how likely is an attack on a SCADA system?

Answer: The Bureau of Reclamation has no specific statistics on probability of attacks against SCADA systems in industry or the federal government at large. Reclamation assumes, however, given the importance of water and power infrastructure, that SCADA could be the target of an attack.

Question: Based on available research, how frequently are SCADA networks attacked?

Answer: The Bureau of Reclamation has no specific statistics on attacks against SCADA systems in industry or the federal government at large. Reclamation has monitoring systems in place and, to date, has not identified any attacks against our SCADA systems throughout the history of their operation. We believe this is due to the isolation of our SCADA systems from the internet.

TOPICS II–IV—No questions pertain to the Bureau of Reclamation

TOPIC V. DAM SAFETY

Question: Does the Bureau of Reclamation monitor only the 17 or so dams that it has created? Or is the bureau monitoring and conducting threat assessments to private dams as well?

Answer: Reclamation has constructed manages 471 dams, 58 hydroelectric powerplants, and other related facilities in the 17 Western states. For security purposes, Reclamation has identified 280 of these facilities as critical for completing security assessments. Reclamation reassesses these facilities on a periodic basis. A security risk assessment examines the threats, vulnerabilities, and consequences of a security event at a facility. Although Reclamation has provided some assistance to other Federal agencies, it does not monitor or conduct threat assessments for private dams.

Question: Help me understand further the way that the control systems at our nation's dams are connected to computers far from the dams and what specific defenses you have put in place to protect those communications links?

Answer: Reclamation uses leased lines and federal microwave channels to address nearly all long-haul communications between SCADA control centers and their outlying controlled sites. This is true of all significant and critical SCADA communications. In some instances UHF or radio communication hops may be employed to support less significant SCADA functionality where data collection and low-risk

control functionality are involved. Short-haul communications employ fiber-optic copper cabling for communication between control system components that are widely distributed geographically. We use federally-owned microwave-based telecommunications systems. In a few cases, we also lease point-to-point circuits from telecommunications companies. These SCADA communications circuits are dedicated (not shared). Reclamation uses several protection methods including non-Internet communications protocols and one-way communications paths. No SCADA system communication takes place over the Internet.

Follow-up Question: Can those connections be used to open flood gates? And if in the when the reservoirs are full, someone did that. would there be a high probability of lives being lost? Have you had damage estimates done at maior Federal dams? Do know how many lives might be lost?

Answer: None of the Reclamation spillway gates under SCADA control have a capacity greater than the safe channel capacity. Therefore, no lives can be lost by flooding outside the safe channel capacity by the mere operation of Reclamation SCADA systems. Instead, Reclamation typically relies on manual, on-site operation of the gates. For the few spillways that are operated with SCADA systems, safety measures are in place. The safety measures in place include: remote monitoring of gate position; control action timing relays that allow only limited raise or lower motion based on a single control action the gate will only raise or lower a certain percentage of its full travel based on one command); and manual SCADA control lockouts that must be physically and procedurally bypassed to enable SCADA control, thereby preventing SCADA control of critical fully supervised. In addition, some gates have limiting switches that only permit them to be moved a small amount at a time.

From our dam safety program, we have estimates for each high and significant hazard dam of population at risk (number of individuals damaged including owned property) and loss of life in the event of complete dam failure. In many cases, we also have estimates of population at risk and loss of life in other flood situations such as failure of gates. We would be willing to give you a secure briefing to provide more information, at your request.

Question: We have heard the story of a hacker control of some systems of the Roosevelt dam in Arizona, which holds 400 trillion gallons of water. What is the worst damage that could be done there? Is it possible to shut out on-site control? In other words, if someone hacked the system and tried to release the water, switch off a hydro-generator, etc., one would assume that there is an on-site, physical override of the SCADA or Process Control System Is that true in all cases?

Answer: It is true that, in 1994, a hacker dialed into a system that monitored the water levels of canals in the Phoenix, Arizona, area. This system was designed for water level monitoring only, and investigators concluded that the hacking incident posed no threat to safety. The story of a 12-year old hacker control of the floodgates at Theodore Roosevelt dam in Arizona in 1998 is, fortunately, only a myth of unknown origin.

The discharge capacity of the one powerplant unit at Roosevelt Dam that can be controlled remotely by SCADA is small and well within the safe discharge capacity of the downstream Salt River. Such a discharge could also be easily handled at Horse Mesa Dam, Mormon Flat Dam, Stewart Mountain Dam, and Granite Reef Diversion Dam, all downstream of Roosevelt Dam. An intruder into the SCADA system cannot cause any releases of water from the dam that will result in any downstream flood damage or threaten the safety of any downstream populations.

SCADA control capabilities can always be disabled at the controlled device (generator, gate, valve, etc.) via a manually operated local control switch.

Question: Are stand-alone networks used at dams, or do you piggyback on the local phone network, the Internet, or some other existing outside network? Is there a Bureau of Reclamation policy on what networks can be used for SCADA/PCS?

Answer: SCADA networks are isolated from networks other than similar SCADA networks. Reclamation's policy addresses all networks (including SCADA) and includes network expansions and extensions, which must be approved by Reclamation's Chief Information Officer. Approval adheres to guidance of the National Institute for Standards and Technology (NIST) and is based on internal vulnerability assessments.

Question: Generally are the Cyber Security requirements of the Bureau of Reclamation department-wide or do have different requirements for each dam? If you have a Bureau of Reclamation Standard, is it the same

as the Army Corps of Engineers, the Tennessee Valley Authority, and other federal agencies/entities?

Answer: Reclamation applies the same baseline cyber security requirements to all of its systems, regardless of the type of system or its location. In some instances, additional security requirements are imposed because of the higher criticality or sensitivity of the information or functions processed by a cyber system. Many SCADA systems fall into this higher criticality or sensitivity category and are consequently held to higher security requirements. In all cases, however, these additional requirements are consistent with NIST and Federal Information Processing Standards (FIPS) guidance.

Although the security foundation requirements for all federal entities are very similar for systems of similar sensitivity and criticality, civilian agencies, such as the Department of the Interior, are subject to the cyber security guidance published by NIST. Agencies under the Department of Defense, such as the Army Corps of Engineers, are subject to a different set of policy, standards, and guidance. Cyber security policy developed by the Department of the Interior and the Bureau of Reclamation will probably not be identical to that prepared by the Army Corps of Engineers, the Tennessee Valley Authority, or other federal entities. The differences, though, are likely to be in details related to meeting mission and organizational needs and requirements, not in foundational cyber security requirements or security best practices.

Question: Do all Bureau of Reclamation dams use the Risk Assessment for Dams to assess the threat, vulnerabilities, consequences, and ultimate risk that the faces?

Answer: Reclamation uses three methodologies depending on facility criticality. For National Critical Infrastructures, Reclamation uses the Defense Threat Reduction Agency assessments. For 50 of our critical facilities, we use the RAM–D methodology. For lower priority facilities, Reclamation uses the Matrix Security Risk Analysis (MSRA)

Question: How Bureau of Reclamation facilities have done RAM–D or other assessments? Have those vulnerabilities been addressed so that security is up to an acceptable level?

Answer: Following the events of 9–11, security was enhanced at all Reclamation facilities, with full time guards and patrols being deployed to the most critical facilities. Reclamation initiated comprehensive security risk assessments at all 280 critical facilities, completing the most critical facilities in 2002 and the less critical ones this past year. The assessments identified potential threats, vulnerabilities, and consequences. The assessments resulted in numerous recommendations for enhancing security through both procedures and facility fortifications. Recommendations for enhancing security procedures were implemented upon completion of the assessments, as they generally did not require new funding. Recommendations for facility fortifications require additional funding, and those are being programmed and implemented on a priority basis. Security fortifications are complete at one National Critical Infrastructure (NCI) facility and in progress at the other and several Major Mission Critical (MMC) facilities. Over 73% of all recommendations resulting from the risk assessments have already been implemented.

Question: Dams are one of the Key Asset Sectors identified in Homeland Presidential Directive 7. Since the issuance of HSPD 7, how much has the Bureau of Reclamation's increased? Have you had to shift spending from other priorities to pay for security?

Answer: Reclamation's enacted and requested security budgets have increased over the FY 2003 appropriated security budget of $28,440,000. Reclamation continues to take its security responsibilities seriously, and aligns security priorities with all other mission critical programs.

Following is a brief summary of Reclamation funding for security for Fiscal Years 2003 through 2006:

FY 2003: $28,440,000 appropriated
FY 2004: $28,583,000 appropriated
FY 2005: $43,216,000 appropriated 2006:
FY 2006: $50,000,000 ($40 million appropriated $10 million from beneficiaries)

RESPONSES FROM DR. SAM VARNADO TO THE HONORABLE BENNIE G. THOMPSON QUESTIONS

I. ***THE THREAT: PROBABILITY/IMPACT OF ATTACKS ON SCADA SYSTEMS***

• (To all) Based on all available research, how likely is an attack on a SCADA system?

The probability of an attack by a dedicated adversary is not known. The probability of nuisance acts, occurring on a daily basis, is 100%.

There is no current, reliable, classified or unclassified estimate of the specific probability of a malevolent attack on SCADA systems. However, we know SCADA systems are vulnerable. We also note an article in the June 27, 2002 *Washington Post* that these systems have been targeted by al-Qa'ida terrorists who have a great deal of capability and patience. There are signs that hacker coalitions and nation states are collecting information on SCADA systems. The sophisticated threats have significant financial resources and can attack at will. Because of the commonality of computing platforms in a networked system, an attack that is successful against one will almost surely succeed against them all, and at only slight additional cost to the attacker.

SCADA systems are now moving from the old stand-alone legacy systems to systems that use the internet or local enterprise networks as the backbone. This means that all the current computer attack modes—worms, viruses, denial of service-can now deny or disable control systems. It is no longer a requirement for a successful attacker to be a control systems expert to bring down a SCADA system. These types of attacks occur daily.

• (To any of the labs) What cyber security failures and incidents have you seen with SCADA networks?

Sandia National Laboratories has performed numerous critical infrastructure assessments that identified common vulnerabilities in SCADA systems. The results are published in a paper entitled "Common Vulnerabilities in Critical Infrastructure Control Systems" that can be found at http://www.sandia.gov/scada/documents/031177C.pdf. This paper describes the types of vulnerabilities we have identified.

In addition to our assessments, there have been the following documented incidents:

> It has been reported that in June 1982, exploitation of SCADA software created a damaging attack on the Trans-Siberian pipeline. The software that was used to run the pumps, turbines, and valves of the pipeline was programmed to malfunction after a specific time interval. The malfunction caused the control system to reset the pump speeds and value settings to produce pressures beyond the failure ratings of the pipeline joints and welds. The result was the largest non-nuclear explosion (3 kilotons) ever seen from space.

In January 2003, the "Slammer" worm disabled a monitoring system at the Ohio Davis-Besse nuclear power plant. The worm entered through an improperly secured network connection to a contractor's facility. The worm crashed the computerized panel used to monitor the plants most crucial safety indicators. This incident did not pose a safety threat at the time because the reactor was offline for repairs and the redundant analog monitoring systems were still in operation. However, this event illustrates the impact that a computer worm can have on a SCADA System. Reference: "Slammer worm crashed Ohio nuke plant network", Kevin Poulsen, Security Focus (19 august 2003): http://www.securityfocus.com/news/6767

In May 2001, attackers were apparently able to gain access to one of the computer networks at the California Independent System Operator (Cal-ISO) corporation. This hacking incident was apparently unsuccessful at penetrating any process control system network, yet it uncomfortably extended over a period of more than two weeks. Reference: "California hack points to possible IT surveillance threat," Dan Verton, Computerworld (12 June 2001): http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html

One verified attack occurred in April 2000 at Maroochy Shire, Queensland. Disruption of the SCADA systems that controlled the plant resulted in release of copious quantities of sewage into parks, rivers, and a hotel, severely fouling the environment. Reference: "Hacker jailed for revenge sewage attacks," Tony Smith, The Register (UK) (31 October 2001): http://www.theregister.co.uk/content/4/22579.html

At about 3:28 PM Pacific Daylight Time on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1.5 hours after the rupture, the gasoline ignited and burned approximately 1.5 miles along the creek. Two 10 year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham's water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least $45 million. The National Transportation Safety Board listed five reasons for the rupture. The fifth was Olympic Pipe Line

Company's practice of performing database development work on the SCADA system while the system was also being used to operate the pipeline, which led to the system's becoming nonresponsive at a critical time during pipeline operations. Reference: http://www.ntsb.gov/publictn/2002/PAR0202.htm

• **(To all) Based on all available research, how frequently are SCADA networks attacked?**

Again, the answer depends in part on how one defines "attack". If attack includes active scanning, attempts to take advantage of unpatched vulnerabilities, worms, viruses, and spyware, then any control system network connected directly or through a business network to the Internet is under constant attack. It is reasonable to assume that network-connected SCADA systems across the country are probed daily.

There have not been many documented malevolent attacks of SCADA or control systems. Attacks do happen, and there are more attacks then we know about because some infrastructure owners are reluctant to report SCADA attacks. They worry about loss of public confidence and competitive issues. We have seen a few targeted attacks in our 10 years of experience.

• **(To any of the labs) Is it possible to devise an attack to disable or disrupt a SCADA network for an extended period of time? If so, what is being done to mitigate such attacks?**

Yes, it is possible to disable or disrupt a SCADA network for an extended period of time. The exact method of attack depends on the individual circumstances of the SCADA network. The Maroochy Shire wastewater SCADA system attack in Australia is often cited because the details are unclassified. Whether one considers the consequences significant or not, the fact remains that disgruntled computer expert Vitek Boden caused a chronic disruption of a SCADA network for three months. His attack could have been more sophisticated and, possibly, might have caused greater consequences. More significantly, the SCADA components he attacked are commonly used in domestic water treatment systems. Sandia's internal research and development has discovered forms of attack that could result in even greater consequences. The details of these attacks are classified and would need to be shared in a different venue.

The responsibility for mitigation is distributed among the SCADA network owner/operators, the SCADA network integrators, the SCADA equipment vendors, industry groups, and regulators. Even when one of the players takes responsibility for security, they can only mitigate the portion they control. Operators can put in place security policies, plans, and implementation, but they are at the mercy of vendors who may not provide features necessary for security. For this reason, the degree of mitigation of SCADA networks is highly variable.

Mitigation effects may not be implemented for several reasons. First, a business case for industry to invest in SCADA security has not been clearly made. As a result, funding for security personnel and equipment are often inadequate.

A second problem is natural attrition through aging of key personnel in utility operations. Taken together, it is probable that quick automation repairs will no longer be possible for many utilities in the very near future, primarily because of a shortage of trained personnel and old equipment. Backup manual operation is further exacerbated by the paucity of skilled and experienced personnel. There are also limitations on the number of field operators, to deploy to remote locations in manual situations when data are unavailable to the SCADA system. Therefore, if the loss of some automation functionality will likely cause severe problems for utility operations (including system management functions, system/plant automated control, or any of the supporting data categories), a redundant system and/or network is required.

Third, classification, anti-trust, and proprietary issues get in the way of the open sharing of threat and vulnerability information among industry stakeholders.

Sandia has been teaching courses on SCADA security assessment and best practices for mitigation to industry and government for several years. In that time, our message has been heard by some entities, who are now asking for more information. We have performed vulnerability assessments that continue to confirm the presence of common vulnerabilities.

• **(To KP Ananth or Sam Varnado) Electric power is important for nearly all the things that Americans do—from businesses to schools to government to many forms of recreation. Has your research shown that the SCADA systems that control our power generation and distribution are fully protected from attacks launched from the Internet? If not, what kind of damage do your researchers believe smart, well researched attacks could cause?**

SCADA networks that control electric power generation, transmission, and distribution are not fully protected from attacks launched from the internet. Well researched attacks can cause burn-out of expensive, hard-to-replace equipment such as transformers. The duration of such outages could extend to several months. Other computer attacks, such as worms or viruses, could create outages lasting for days.

Further information about the consequences of a smart, well-researched attack is available at a classified level and could be provided in another venue.

• **(To Sam Varnado, KP Ananth, Bill Rush) We've heard a lot about the impact of a terrorist attack on a control system. But as we saw during Katrina, natural disasters can cause devastating impacts to our control system infrastructure too. What kind of impact would a natural disaster have on control systems in California (earthquakes), Oregon (tidal waves/tsunamis), the Gulf Coast (hurricanes), and elsewhere?**

Terrorist attacks differ from natural disasters in that the terrorists take a functional attack perspective. In other words, they look to destroy or alter the functionality of a SCADA system. In contrast, a natural disaster is random and geographically dependant. Anything within the physical range of the disaster is affected. Anything outside is less likely to be affected. Many companies have created redundant control centers to better prepare for such disasters. The critical assets are identified and duplicated, and risk-mitigation plans are usually in effect.

In some respects, certain natural disasters are easier to handle than focused cyber attacks. A crew made up of control specialists and physical facilities members can very quickly determine what physical assets have been damaged. These assets can be reordered and replaced like any other field equipment. Typically, control systems are composed of off-the-shelf parts and reordering is not usually a problem.

Lack of warning is one aspect that makes response to some disasters more difficult. Hurricanes are different than earthquakes, tsunamis, and terrorist events. Damage can be minimized if there is enough warning to allow shut down. When the event happens with little or no time to prepare, the chance for damage increases. Listed below are the areas of concern, the disaster being considered, and the potential impact.

Gulf Coast:
Natural Disaster: Hurricane
Infrastructure: Oil, Gas, chemical, electrical
Impact: Because of pre-warning, these infrastructures are reasonably well equipped to deal with the disaster. Control system equipment can be damaged or destroyed, resulting in outages of service. However, if the infrastructure elements are shut down prior to the storm, damage can be minimized.

California:
Natural Disaster: Earthquake
Infrastructure: Oil, Electricity, Telecommunication, Natural Gas
Impact: Without warning, many of the infrastructure control systems could be severely damaged through physical destruction of computer facilities. Impacts could be severe and widespread. However, backup systems located in unaffected areas will help minimize the impact and help in system recovery.

Oregon:
Natural Disaster: Earthquake, Tidal Wave
Infrastructure: Oil, Electricity, Natural Gas
Impact: Tidal waves are of less concern than earthquakes. Most infrastructure assets are well protected from tidal waves by landmasses, but they lie in a critical area for earthquakes. Loss of electricity because of extensive physical damage could lead to failures in other infrastructures because they need electricity in order to safely shut down. In addition, the economy in the pacific Northwest could be severely impacted if electrical failures caused a disruption of port activities.

The Department of Homeland Security's (DHS's) Infrastructure Simulation and Analysis Center (NISAC) at Sandia has created a number of relevant reports on the economic consequences of natural disasters as follows:

- Numerous Katrina reports on damage from Katrina both before and after land fall
- A report entitled "Infrastructure Assets in Seismically Active Zones in the Pacific Northwest"; this report addresses assets located in Washington, Oregon, and Idaho
- Analysis of economic impacts of port disruptions in the Pacific Northwest.

Natural disasters affect all critical infrastructures. The interdependent nature of the infrastructure amplifies the consequences of disruption in any one sector. Fortunately, preparing for the abnormal natural disaster event also helps prepare for the

malevolent attack. Many of the practices that Sandia teaches in our course on sustainable security are equally applicable to sustaining operations during natural disasters and recovering after those disasters.

II. *THE PUBLIC/PRIVATE RELATIONSHIP IN DEVELOPING A SCADA SOLUTION*

- **(To any of the labs) I understand the National Labs are conducting extensive research into SCADA and control systems. What resources are you currently lacking? How are you coordinating these efforts with the private sector? What can the federal government do to provide you with more resources?**

Our biggest need is predictable, sustainable, multi-year funding tied to a well-defined research and development plan. We have outstanding well-trained staff who are experts in cyber security. However, cyber research has not been emphasized by DHS. DHS should ensure that the best technical capability in the country is applied to this problem. The national labs—particularly Sandia and Idaho national laboratories—have the necessary talent, but DHS needs more funding to apply to the problem.

In addition, existing DHS programs, emphasize the conventional hacker threat. There is a need to address the more sophisticated threats such as those coming from terrorists and nation states. Sandia has outstanding capabilities in these areas, but they are not being applied to the SCADA problem.

- **How are you coordinating these efforts with the private sector?**

We are currently working with DOE and private industry to develop a roadmap for securing the nation's energy infrastructure from the cyber threat. In addition, we currently engage in a variety of outreach and awareness activities, including teaching vulnerability assessment and SCADA security courses to industry, making technical presentations, and providing the products of our research on a website, http://www.sandia.gov/scada/. We participate in programs such as the Institute for Information Infrastructure Protection (I3P), Linking the Oil and Gas Industry to Improve Cyber Security (LOGI2C), Process Control Systems Forum (PCSF), and the National SCADA Test Bed (NSTB); all are aimed at fostering cooperation and coordination with industry. We also frequently host visits from industry to Sandia.

Additionally, we provide training on risk assessment methodology and vulnerability mitigation to a wide range of industrial customers.

- **What can the Federal Government do to provide you with more resources?**

Funding should be increased for improvements in cyber security technology so that DHS can provide tools for

- high speed intrusion detection systems
- software assurance
- attack attribution and trace-back
- security modeling of existing and proposed SCADA systems
- network visualization for mapping cyber disruptions
- triage of threat scenarios across many vectors
- assuring the reliable performance of commercial off-the-shelf (COTS) products. We need funding of $15M/yr to apply to this problem
- models and simulations to understand the large-scale, transient consequences of attacks on the power grid.

Funding for a new program to address the sophisticated threat should also be provided. We anticipate that more sophisticated and strategically integrated cyber attacks—such as those that might be marshaled by a well-funded and highly capable terrorist or nation-state actor—will occur against control systems. An effort is needed to develop the analytic resources and technologies required to detect and predict these threats based on control system vulnerabilities, to strengthen our preventive measures, to increase our ability to respond expediently, and to model these more sophisticated threats and analyze the operational impacts they have on control systems. In general, this is a better role for national laboratories than for universities and private industry vendors. Sandia could lead this program. This effort should include a strong emphasis on the problems of building trusted systems from untrusted COTS components.

Further, we need funds to work more closely with industry to provide in-depth vulnerability assessments of existing systems, to help industry utilize existing risk assessment models, and to formulate a business case for investment in cyber security.

Finally, DHS needs to identify the commonalties in SCADA systems across all infrastructure elements and then define and coordinate efforts for improving SCADA

system security across these infrastructures. Industry infrastructures owners should be provided a single point of contact for their interactions with DHS.

- **(To any of the labs) It has been widely reported that both industry and the federal government find it difficult to estimate the economic impact of a cyber security attack. Has the lack of actual quantifiable damages made the private sector leery of investing in cyber security?**

At the I3P SCADA Security Conference in June 2005, held in Houston, panelists from industry made exactly this point. They said:

> "The lack of quantifiable damages is one of the missing components that would feed into the private sector's cost-benefit and return-on-investment analysis. The economic case for investing in cyber security has to be stronger than the economic case for investing in anything else before the private sector will be compelled to make cyber security investments."

This observation illustrates the difficulty that industry is having in making a business case for investment in cyber security. There are two steps that will help overcome the noted deficiency. First, DHS should fund the national laboratories to work with industry in utilizing the lab's risk assessment methodology to help industry make the business case. Second, DHS should apply the skills of NISAC, run by Sandia and Los Alamos labs, to the problem of determining the economic consequences of infrastructure outages caused by cyber attacks.

- **(To Sam Varnado, KP Ananth, Bill Rush) Can you tell us specifically how your research on SCADA has, to date, impacted the way SCADA systems in the field are secured, and what percentage of those systems have been impacted? If that's not a big number, what is stopping us from putting the results of your research into practice in the field?**

We have directly affected relatively few systems, on the order of tens. Unfortunately, our program is small and the number of control systems is huge. We have indirectly affected—either by developing self-assessment methodologies or through outreach—on the order of hundreds of control systems. We have diffused our standards work to thousands of control systems. In spite of such efforts, we have only affected a small fraction of the control systems on which the nation depends for its current infrastructure security.

The biggest obstacle to technology transfer is the business case issue. Even when industry believes there is a business case for security measures, they believe that they need only increase security enough to protect against the low-level threat—background noise, individual hackers, and possibly hacktivists. It is industry's contention that government should protect against the larger threats—organized crime, terrorists, and nation-state threats—either through law-enforcement or national defense. We need to expand our public/private partnerships to define best industry practices as a function of risk and cost, then develop and disseminate the appropriate technology.

- **(To Sam Varnado, KP Ananth, Bill Rush) What has the money we have already spent on SCADA research done to improve SCADA security in the field?**

A specific instance of improved SCADA security is the work conducted to develop RAM–W, a self-assessment methodology for water utilities. Hundreds of water utilities used that methodology to help secure their SCADA systems. One particular utility, Washington Aqueduct, operated by the US Army Corp of Engineers, has benefited directly from the assessment and the secure design requirements that Sandia provided for their new SCADA system as a follow-on project.

We have been active in international standards organizations by helping to provide a security perspective to their guidelines, by developing training classes, and by developing self-assessment methodologies. We have also developed technology to secure communication links and improve cryptographic research.

We have published and distributed to industry a report entitled "Common Vulnerabilities in Critical Infrastructure Control Systems." We have also provided training courses to industry on vulnerability assessments of SCADA systems as well as risk assessment methodologies to help industry solve its own problems.

Further, we have identified specific vulnerabilities in SCADA systems from several vendors. We have also explained to those vendors how the vulnerabilities can be mitigated.

Over the last ten years, Sandia has invested in SCADA security research, through its own internal research and development funds, on the order of $4 million. Currently we are funded through external sources—DHS, DOE, industry, and university collaborations—at approximately $3 million this fiscal year. This level of fund-

ing is not adequate to address the very hard problems that SCADA security presents.

- **(To Sam Varnado, KP Ananth, Bill Rush) Is there any risk of duplicating efforts with the lab beds at Sandia and Idaho and other research around the country?**

There is no duplication. The efforts are complementary, with each lab applying its unique capabilities to different parts of the problems.

The test bed at Idaho National Laboratory is designed to demonstrate the effects of cyber attacks on large scale physical structures. It is a unique facility.

The test bed at Sandia is in reality a SCADA security laboratory that conducts leading-edge research on cyber security methods such as vulnerability assessments, cryptography, security of wireless networks, and threat analysis. It provides the capability to test the robustness of SCADA systems from various vendors in a laboratory environment at low cost. It is also set up to evaluate the more sophisticated adversaries.

Further, DHS manages the work at both labs and provides a program manager to make sure tasks are assigned in a way that avoids duplication. It is important that DHS understands and acknowledges the uniqueness of each lab and works to make sure that the participants at one lab do not duplicate existing capabilities at the other lab.

III. ***THE FEDERAL GOVERNMENT'S ROLE IN CYBER SECURITY***

- **(To Andy Purdy and ALL) There are several SCADA test beds across the country. Is there any risk of duplicating efforts with the lab beds at Sandia and Idaho and other research? Is there any way to consolidate these efforts?**

See our answer on duplication under the preceding question.

Consolidating these facilities does not make sense because they have separate roles. One is a large, full-scale test and demonstration facility; the other is a state-of-the-art research facility needed for developing countermeasures for the increasingly sophisticated threat environment.

IV. ***THE FEDERAL ROLE IN THE FUTURE***

- **(To Sam Varnado and K.P Ananth) Based on your knowledge of the SCADA research field, what are the most promising technological breakthroughs you see that can protect our SCADA systems in the short term? I realize there are no silver bullets, but please list the solutions that will actually work to protect our SCADA systems.**

First, industry infrastructure owners need to define security policies and best practices for their own systems. Security is not just a technology problem. It is one of sustainable security—hardware, software, people, and procedures. Employees need to be trained in detecting attacks. Widespread adoption of best security practices has high payoff and low costs. If all control systems implement best security practices, the bar will be raised against all adversaries.

Second, the latest security advances such as intrusion detection systems, firewalls, encryption, and other technologies should be applied. For example, the application of new Layer 3 firewalls in switches is emerging and shows promise for improving the security of control systems.

Third, vulnerability assessments need to be performed on all major SCADA systems. Then the identified vulnerabilities need to be mitigated.

Finally, a strong, sustainable R&D program needs to be implemented to continue to develop technology for countering new, more sophisticated threats by hackers and cyber terrorists who change their attack methods on a very frequent basis.

- **(To any of the labs) How do we make rapid progress in improving security in the field?**

We must help infrastructure owners develop security policies and train their people.

We must provide incentives and liability relief to developers and adopters of security technology. The Safety Act is a good step in this direction.

We must support more research into robust, distributed, introspective systems; more research into secure operating systems; and—to achieve a high level of security—implement a dedicated internet protocol (IP) and a redesigned IP stack for SCADA use only.

We must enable greater access to, and partnerships among, vendors, labs, and asset owner/operators in order to better understand industry facilities, processes, and more technology from the labs to the field.

We must provide better and clearer communication among organizations working on cyber security to help us develop consensus on the best security solutions. We

must also promote opportunities to provide awareness and training to vendors and asset owner/operators.

• **(Any of the labs) Has the federal government advocated for standards establishing a minimum floor for securing control systems? What would a minimum floor look like? Have industry leaders begun the process of developing those standards already? Has the government established any "best practices" that can be modeled by industry? What other standards activities are being developed besides AGA 12?**

To our knowledge, three government initiatives exist today to address securing control systems by providing guidelines and/or cyber security requirements to industry: (a) the Technical Support Working Group (TSWG) "Securing Your Industrial Control System" guide book; (b) the NIST release of the "Guide to Supervisory Control and Data Acquisition and Industrial Control System Security"; and (c) the DHS US-CERT Control Systems Security Center (CSSC) Program cyber security protection framework, which includes a set of cyber-security requirements planned to be released in 2006. Whether these individual government released documents constitute a "minimum level of standards/guidelines" is not clear.

From our experience, a minimum set of security control system standards would not come from a single standards body but would most likely comprise the work of various standards bodies. There is no single standards body to provide a comprehensive list of control systems cyber security standards.

Industry-led standards bodies have begun developing standards to address the issue of securing control systems. However, dozens of groups/organizations currently exist that are working on control systems security standards. Coordination of these efforts is both essential and, at the same time, difficult. Inconsistent and conflicting standards generated from these various groups confuse industry and asset owners/providers. A more concerted effort on the part of the government is needed to assist industry and asset owners in (1) maneuvering through the abundance of control systems cyber security standards and (2) encouraging them to develop consistent control systems cyber security standards across all critical infrastructure sectors. A single point of contact within DHS for cross-sector involvement in control systems cyber security standards is needed. This point of contact would facilitate and assist in directing industry partners to relevant security guidelines, practices, and standards, and it would encourage consistent application of cyber security standards.

Other standards bodies include API 1164, CIDX, FIPS Pub 200, ISA SP99, NERC, and NIST SP800–53—as well as others too numerous to list. The international standards bodies (e.g., IEC) are an important group because the majority of SCADA vendors are international and follow those guidelines.

• **(To any of the labs) Some have mentioned the value of a "vendor" incentives system that would provide tax and other financial incentives to manufacturers who are producing control systems that are already in "best practice" compliance. How feasible is this, and have there been evaluations of the cost to the federal government?**

Best practice compliance can be conducted at a component or sub-system level if clear metrics are established to define the practice. But even here care must be taken not to impose a standard on something that a later technology might supersede. Cyber security technology is a rapidly changing field.

Great care would need to be taken to insure that the "best practice" standards would not be negotiated down to the point that companies just need to fill out the right forms and jump through the right legal hoops—doing little to actually improve security. A third party, Underwriter's Laboratory approach may be necessary to properly evaluate vendor's products and validate claims. Some analysis should also be performed to determine the appropriate incentives for compliance (industry, company, product, etc.).

○