AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING THE ELECTRIC GRID FROM CYBERSECURITY THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY AND AIR QUALITY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

SEPTEMBER 11, 2008

Serial No. 110–145

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

61–860 PDF WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
DORIS O. MATSUI, California

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
BUD ALBRIGHT, *Minority Staff Director*

SUBCOMMITTEE ON ENERGY AND AIR QUALITY

RICK BOUCHER, Virginia, *Chairman*

G.K. BUTTERFIELD, North Carolina, *Vice Chairman*
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
ALBERT R. WYNN, Maryland
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
DORIS O. MATSUI, California
JOHN D. DINGELL, Michigan *(ex officio)*

FRED UPTON, Michigan *Ranking Member*
RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
ROY BLUNT, Missouri
MARY BONO MACK, California
GREG WALDEN, Oregon
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas *(ex officio)*

PROFESSIONAL STAFF

SUE D. SHERIDAN, *Chief Counsel*
JOHN W. JIMISON, *Counsel*
RACHEL BLESHMAN, *Legislative Clerk*
DAVID MCCARTHY, *Minority Counsel*

CONTENTS

	Page
Hon. Rick Boucher, a Representative in Congress from the Commonwealth of Virginia, opening statement	1
Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement	13
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachussetts, opening statement	13
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	14
Hon. Mike Rogers, a Representative in Congress from the State of Michigan, prepared statement	16
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, prepared statement	128

WITNESSES

James R. Langevin, Chairman, Subcomittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security	19
Prepared statement	22
Joseph Kelliher, Chairman, Federal Energy Regulatory Commission	36
Prepared statement	39
Answers to submitted questions	145
Kevin M. Kolevar, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy	45
Prepared statement	48
Answers to submitted questions	164
Richard P. Sergel, President, North American Electric Reliability Corporation	64
Prepared statement	67
Answers to submitted questions	176
Susan N. Kelly, Vice President, Policy Analysis, and General Counsel, American Public Power Association	78
Prepared statement	81
Answers to submitted questions	178
Steven T. Naumann, Vice President, Wholesale Market Development, Government and Environmental Affairs and Public Policy, Exelon Corporation	93
Prepared statement	95
Answers to submitted questions	183
Barry R. Lawson, Manager, Power Delivery, National Rural Electric Cooperative Association	107
Prepared statement	109
Answers to submitted questions	188

SUBMITTED MATERIAL

Discussion draft	4
National Association of Regulatory Utility Commissioners, NARUC, statement of, submitted by Mr. Boucher	129
Electricity Consumers Resource Council, ELCON, statement of, submitted by Mr. Boucher	134
Canadian Electricity Association, CEA, statement of, submitted by Mr. Boucher	138
Subcommittee exhibit binder index	144

PROTECTING THE ELECTRIC GRID FROM CYBERSECURITY THREATS

THURSDAY, SEPTEMBER 11, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY AND AIR QUALITY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:10 a.m., in room 2322 of the Rayburn House Office Building, Hon. Rick Boucher (chairman) presiding.

Members present: Representatives Boucher, Melancon, Barrow, Markey, Upton, Shimkus, Walden, Rogers, and Barton (ex officio).

Staff present: John Jimison, Richard Miller, Rachel Bleshman, Alex Haurek, David McCarthy, Andrea Spring, and Garrett Golding.

OPENING STATEMENT OF HON. RICK BOUCHER, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. BOUCHER. The subcommittee will come to order. This morning we are addressing a means of protecting the Nation's electricity grid from cybersecurity threats through which computer hackers could maliciously gain access by way of the Internet to the computers controlling key components of our Nation's electricity system and cause either short term system outages or more serious permanent system damage.

No industry is more essential to the Nation's economy than is our electricity sector, and its protection is vital to both our economic security and to our national security. The Nation's electricity system consists of generators and regional networks of interconnected transmission lines. The controls which operate the grid and electricity generators attached to it are increasingly computer-connected to the Internet.

In fact, increasing the degree of interactive grid computerization is a major element of the development of a smart grid which will improve system reliability, optimize generation, promote load balance, improve consumption management, and integrate new smart appliances and equipment. But with increased reliance on interactive digital technology comes the added risk of computer hackers entering the system and causing truly extensive damage.

The Idaho National Laboratory conducted tests using the code name Aurora, demonstrating that standard utility control systems could be penetrated and adversely affected through unauthorized computer access. This demonstration showed that a cyber intruder

could manipulate the control systems of a generation facility resulting in massive physical damage that could take months to repair.

Cyber attacks on electricity systems have occurred in a number of nations, and the Federal Energy Regulatory Commission reports 20 documented cases where hackers have penetrated networks and were able to affect controls on dams, on a nuclear reactor, and have disabled backup generation and shut down power plants. The Defense Science Board reports that U.S. grid control systems are continuously probed electronically, and while none has yet been the subject of major damage or grid outages in the United States, cyber attacks have caused major grid outages in other nations.

In 2007, the Department of Homeland Security notified the North American Electricity Reliability Corporation, known as NERC, of the Aurora vulnerability demonstrated by the Idaho National Laboratory. Based on this notification, the NERC issued an advisory to 1,800 owners and operators of facilities associated with our Nation's power grid and provided a 60-day schedule for immediate mitigation measures as well as longer term measures that would be implemented over a 180-day period.

But compliance with this advisory recommendation was entirely voluntary by these 1,800 owners of facilities that are components of the national grid. The Federal Energy Regulatory Commission recently audited compliance with the advisory issued by the NERC and conducted that audit among 30 utilities. It found that of the 30 audited, 23 were not in compliance with the NERC advisory. One utility reportedly had a 10-year compliance schedule, notwithstanding the fact that 180 days was the outer limit for compliance in the NERC advisory.

Another utility had never changed the factory-installed user names and passwords on its computers controlling its systems, and it was therefore clear that self-interest alone was not a sufficient motivation to mitigate the Aurora vulnerability.

Based on the documented threat to the electricity system and on the noncompliance with voluntary measures which the audit revealed, the FERC, along with the U.S. Department of Energy and the Department of Defense, have identified an urgent need for legislative authority to allow the federal government to compel implementation of the measures to respond to the cybersecurity threat to our Nation's electricity grid.

In response to that need, this subcommittee, on a bipartisan basis, has developed a bipartisan discussion draft. It requires the FERC to undertake a rulemaking to determine what measures or actions should be required to protect the bulk power system against vulnerabilities and then provides the FERC with the authority to enforce the rule once adopted.

In addition, the FERC would be granted authority to issue such emergency orders as it deems necessary to protect the reliability of the bulk power system with regard to potential new cybersecurity emergencies not identified in the original rule, which are judged to be imminent threats under presidential declaration.

While the discussion draft represents an outstanding bipartisan step toward enactment of the necessary federal legislation, several questions do remain open, and these questions will be addressed by our witnesses this morning. The outstanding issues include wheth-

er any legislation should be limited to cybersecurity threats alone or whether a grant of authority to address physical attacks on the grid should also be included.

Another open issue is the exact wording of the specific definition of cybersecurity threat. A third open issue is the set of circumstances under which interim measures may be discontinued once they are activated. And finally the scope of the bill with regard to whether it includes entities not technically within our bulk power system, such as the electricity systems of the States of Hawaii and Alaska, the territory of Guam, and also core distribution facilities for electricity in some of our major cities such as New York City and Washington, D.C. And we will hear from our witnesses with regard to their sometimes contrasting views on these outstanding issues.

Today's hearing will feature expert witnesses who will present information on both the potential threat of cybersecurity attacks against the electricity system and also the appropriate legislative response that we should be making to guard against those threats.

I want to commend the staff on a bipartisan basis for the outstanding work that they have done during the August recess on this matter. The staff on both sides of the aisle have participated together in obtaining briefings from the agencies I have identified in this statement. They have participated together in constructing the legislative draft that is the subject of our hearing this morning, the discussion draft. And I want to commend them for doing that at a time when Congress was not here and when they were busily at work attending to this urgent business.

I also want to say thank you to the ranking member of this subcommittee, Mr. Upton from Michigan, for his outstanding efforts and for that of his staff. He and I have had discussions with regard to this matter. We are participating jointly in the exercise to move our discussion draft to final legislation and to markup. Hopefully that will occur perhaps within the course of the coming week.

And that partnership is a reflection of how this subcommittee and our full committee operate when it is at its best, and that is working in a bipartisan fashion to produce consensus solutions to the major problems that confront us. Nowhere has that effort been better reflected than in the work that has been done over August and that we continue here this morning.

[Discussion draft follows:]

STAFF DISCUSSION DRAFT

[This discussion draft highlights the remaining areas of disagreement. Language not highlighted has been tentatively agreed to by FERC representatives and the industry associations that have participated, pending full agreement.]

110TH CONGRESS

2D SESSION **H. R. _____**

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity [FERC: and other national security] threats to the reliability of the bulk-power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. _____ introduced the following bill; which was referred to the Committee on _____.

A BILL

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity [FERC: and other national security] threats to the reliability of the bulk-power system, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Bulk Power System Protection Act of 2008''.

SEC. 2. FINDINGS.

The Congress finds that:

(1) it is in the public interest to require the Federal Energy Regulatory Commission to promptly order measures to address known cybersecurity threats to the reliability of the electric bulk power system; and

(2) the Commission must have the necessary emergency authority to respond promptly to future cybersecurity [FERC: and other national security] threats that could compromise reliability of the bulk power system.

SEC. 3. PROTECTION OF BULK POWER SYSTEM FROM CYBERSECURITY [FERC: AND OTHER NATIONAL SECURITY] THREATS.

Part II of the Federal Power Act is amended by adding the following new section after section 215:

''SEC. 215A. EMERGENCY AUTHORITY TO ADDRESS CYBERSECURITY [FERC: AND OTHER NATIONAL SECURITY] THREATS TO THE BULK POWER SYSTEM.

''(a) DEFINITIONS.—For purposes of this section:

''(1) The terms 'reliability standard' ,'bulk power system', 'reliable operation', cybersecurity incident', 'Electric Reliability Organization' , 'regional entity' , and 'owners, users or operators' shall have the same meaning as when used in section 215.

''(2) The term 'cybersecurity threat' [FERC: means that there is credible information or evidence of (1) the likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; or (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act.] [Assns: means that there is credible information or evidence of: (1) the substantial likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; and (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act].

''(3) The term 'national security threat' means a threat to the bulk power system identified by and Federal law enforcement, national security, or intelligence agency of the United States. [Assns would delete this definition]

'(3) The term 'security-sensitive information' means information that, if revealed to the public, could reasonably be expected to have a significant adverse effect on the health or safety of the public or the common defense or national security. The Commission may designate information as 'security sensitive information' for purposes of this section in consultation with national security or national intelligence agencies, as appropriate, but may not designate as security-sensitive information any information that has been classified by another Federal agency.

"(b) INTERIM AUTHORITY TO ADDRESS EXISTING [Assns: CYBERSECURITY] THREATS.—

(1) After notice and opportunity for comment, and after consultation with appropriate governmental authorities in Canada and Mexico [FERC: (subject to adequate protections against inappropriate disclosure of security-sensitive information)] [Assns: (subject to adequate protections against public disclosure of security-sensitive information)], the Commission shall establish, by rule or order, within 120 days of enactment of this section, such measures or actions as are necessary to protect the reliability of the bulk power system against the cybersecurity threats resulting from: (i) the vulnerabilities identified in the June 21, 2007 communication to certain "Electricity Sector Owners and Operators" from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information Sharing and Analysis Center, and (ii) related remote access issues. Such measures or actions may be required of any owner, user or operator of the bulk power system within the United States.

2) Until such time as the interim reliability measures or actions ordered under this subsection are replaced by cybersecurity reliability standards developed, approved and implemented pursuant to section 215, the Commission may issue additional orders to supplement the initial rule or order issued under this subsection only if, based on subsequent information or petition from an affected entity, the Commission determines that clarification or refinements to the originally ordered measures or actions are necessary to ensure that the threats are adequately and appropriately addressed. Any such additional orders shall be preceded by notice and opportunity for comment.

"(c) FUTURE EMERGENCIES INVOLVING IMMINENT CYBERSECURITY THREATS AND CERTAIN OTHER THREATS TO RELIABILITY. [Assns would delete "and certain other threats to reliability"]

"(1) AUTHORITY TO ADDRESS IMMINENT [Assns: CYBERSECURITY] THREAT.— Whenever the President issues and provides to the Commission (either directly or through the Secretary of Energy) a written directive or determination that an imminent cybersecurity, [Assns would delete the following: , or other national security,] threat to the reliability of the bulk power system exists, the Commission may on its own motion, with or without notice, hearing, or report issue such orders for emergency measures or actions as are necessary in its judgment to protect the reliability of the bulk power system against such threat

"(2) CONSULTATION.—Before acting under this subsection, to the extent feasible, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with appropriate governmental authorities in Canada and Mexico [FERC: (subject to adequate protections against inappropriate disclosure of security-sensitive information)] [Assns: (subject to adequate protections against public disclosure of security-sensitive information)], , entities described in paragraph (3), and officials at other Federal agencies,

including the Secretary of Energy, as appropriate, regarding implementation of measures or actions that will effectively address the identified threat[Assns would delete the following: and protect national security.]

"(3) APPLICATION OF EMERGENCY MEASURES.—An order for emergency actions or measures under this subsection may apply to the Electric Reliability Organization referred to in section 215 or a regional entity with respect to the United States operations of the Electric Reliability Organization or the regional entity, or any owner, user or operator of the bulk power system within the United States.

"(d) DISCONTINUANCE.— The Commission shall issue an order discontinuing any measures or actions ordered under subsections (b) or (c) upon the earliest of:

"(1) when the President (either directly or through the Secretary of Energy) issues a written order or directive provided to the Commission to the effect that the threat to the bulk power system that requires such measures, or actions no longer exists;

"(2) when the Commission determines in writing that the ordered measures or actions are no longer needed to address the identified threat;

"(3) when a reliability standard developed and approved pursuant to section 215 is implemented to address the identified threat; or

"(4) [FERC: with respect to orders under subsection (c), one year after the issuance of an order unless the President (either directly or through the Secretary of Energy) issues a determination reaffirming the

continuing nature of the threat, provided that the determination issued under this paragraph shall expire upon the implementation of a standard under section 215 to address the identified threat.] [Assns: one year after the issuance of an order under subsections (b) or (c) unless the President (either directly or through the Secretary of Energy) issues a determination reaffirming the continuing nature of the threat, provided, however, that the determination issued under this paragraph (D) shall expire upon the implementation of a standard under section 215 to address the identified threat.].

The Commission shall issue such order to be effective within 30 days of the relevant triggering event set out in subsections (1) through (4).

"(e) PROTECTION OF SECURITY-SENSITIVE INFORMATION.—

"(1) NONDISCLOSURE OF SECURITY-SENSITIVE INFORMATION.—Notwithstanding any other provision of law, if a rule or order issued under subsection (b) or (c) contains security-sensitive information or if information in the record associated with such rule or order constitutes security-sensitive information, the Commission may make the rule, order or information non-public in whole or in part. The Commission may disclose such non-public rule, order or information to entities other than the recipient of the rule or order as the Commission deems necessary as needed to carry out the rule or order and protect the reliability of the bulk-power system or for purposes of judicial review.

"(2) CONFIDENTIALITY PROCEDURES.— The Commission shall develop procedures

(i) for maintaining confidentiality of security-sensitive information contained in any document or pleading filed with the Commission in response to a proceeding initiated under, or a rule or order issued under, subsection (b) or (c) and may make non-public, in whole or in part, any document or pleading containing security sensitive information. The Commission may disclose all or any part of such document or pleading as necessary to carry out a rule or order under this section and protect the reliability of the bulk-power system or for purposes of judicial review; and

(ii) governing the confidentiality of information deemed to be security-sensitive. The procedures developed by the Commission shall ensure, to the extent consistent with national security, that information may be shared by entities subject to Commission action under this section with their employees, contractors and third-party representatives (including trade associations), to the extent necessary to enable such entities to implement Commission orders or measures and to protect their rights, including the right to judicial review.

Such procedures shall be issued in an order of the Commission on an interim basis after consultation with affected entities and their representatives and shall subsequently be subject to a rulemaking initiated within 120 days of the date that the interim rules take effect.

"(f) REVIEW.— The Commission will act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section which are filed under section 313(a). Any person or other entity seeking judicial review pursuant to section 313 may obtain such review only in the United States Court of Appeals for the District of

Columbia Circuit. In the case of any petition for review involving rules or orders containing or relating to security-sensitive information, the Commission and parties must develop with the court appropriate measures to ensure the confidentiality of such information, including, but not limited to, court filings under seal or otherwise in non-public form, or judicial review in camera.

(g) Enforcement Discretion. The Commission shall exercise its discretion in engaging in enforcement actions under this section to recognize good faith efforts to comply with directives of the Commission.

[Amend Section 201(b)(2) – add "section 215A" to the listing of applicable sections.]

Mr. BOUCHER. And at this time, I am pleased to recognize the ranking Republican on the Energy and Air Quality Subcommittee, Mr. Upton of Michigan, for his remarks.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, and I do want to thank you and the staff on both sides. This is a very important hearing, an issue that we need to deal with. I appreciate our witnesses joining us this morning as well.

Many of us know that the House Homeland Security Committee has examined the issue. They have focused on a vulnerability in electric generator control systems, which could allow remote access, enabling a bad actor or terrorist to remotely destroy a generator.

And today we are going to follow up on those hearings and seek additional answers with a focus on the most productive way to ensure the security of our energy infrastructure. Members of this committee will follow up next week with a classified briefing on the topic as well. And following that briefing, I know that we can work together on bipartisan legislation. I would commend both Mr. Dingell, Mr. Barton in their efforts to that end.

Major questions do need to be addressed. Is there an actual threat capable of causing catastrophic damage? Is there a regulatory gap that needs to be filled? Which agency should take the lead? And I hope that our witnesses will help address those questions today.

Security of our Nation's energy infrastructure from attack is one of these most important issues that our committee will address. This is not an issue that we can take lightly or cover it up in just one hearing. Energy has been one of the leading issues debated in the Congress this year and rightfully so. Energy literally powers our economy. Even small price spikes in supply disruptions can have a large, important economic impact. It is imperative that the security of our Nation's energy infrastructure gets the attention that it deserves.

I look forward to working with all my colleagues to address this in a most beneficial way. And, Mr. Chairman, I would yield back the balance of my time.

Mr. BOUCHER. Well, thank you very much, Mr. Upton. And again I thank you for the outstanding cooperation you and your staff have provided on this matter. The gentleman from Massachusetts, Mr. Markey, is recognized for 3 minutes for an opening statement.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Thank you, Chairman Boucher, for holding this important hearing today and having it on 9/11, the seventh anniversary of that horrific event. It serves as a stark reminder that addressing the vulnerability of cyber threats is long overdue.

We have seen the reality of these incidents in various settings over the years, including the slammer worm at the Davis Besse Nuclear Power Plant and the Aurora vulnerability exposed at the

Idaho National Laboratory. We know that this threat is real. We also know the impacts are real and potentially devastating.

The Northeast blackout in 2003, when an estimated 50 million people lost electricity, is estimated to have cost up to $10 billion and eight lives. And we also know the impacts of these events are the same regardless of whether the incident is caused by someone who wants to do us harm or someone who simply doesn't know they are about to.

But this hearing is timely for other reasons as well. This Nation is finally, after years of control and of pocket padding by the oil industry, gathering the momentum to transition away from a dependence on foreign oil. It is a long overdue transition, and every day that we wait to rechart our course is a lost day. Based on the knowledge we have gained through hours of hearings in Congress, we know that the grid stands as one of the best and most immediate solutions to this crisis. With the surge in interest in alternative energy sources tapping into the grid and the increasing use and promise of electric vehicles, the grid is vital to our move towards energy independence. But it can only serve in this critical role if it is protected as a crucial asset.

Fundamental changes to the structure of our grid could also eliminate or reduce cyber threats or diminish the harm resulting from them. Features offered through the developing smart grid technology, for example, could be used to reduce this threat and better position our response to such an event should such a cyber attack occur. Likewise, more distributed generation could conceivably reduce the extent of the impacts of a cyber attack.

I thank you, Chairman Boucher, for having this hearing. It is obvious that the technologies that affect the two wires or the three wires that go into everyone's home, the cable, the phone company, and the electric company are now all merging in terms of the technologies. And one can help the other, and the other can help the one as we learn how to use technology, both to advance our energy independence agenda and at the same time, ensure that we are being protected from homeland security threats.

So I thank you for being here. I see Jim Langevin down there, my good friend. We welcome you here as well, and I yield back the balance of my time.

Mr. BOUCHER. I thank you very much, Mr. Markey, and, as you have noted, this issue is at the focal point of several issues in which you and I have a common interest, and that is information technology policy as well as energy policy. And I very much welcome your remarks today. The gentleman from Texas, Mr. Barton, the ranking Republican member of the full committee, is recognized for 5 minutes.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman. I just returned from the 9/11 ceremony out at the Pentagon. There couldn't be a better time to hold this hearing on cybersecurity. As we memorialize those brave men and women who gave their lives on September 11, both at the Pentagon and at the World Trade Center and in the fields

of Pennsylvania, we have a real threat against the United States of America.

It is not going away, and we need to defend ourselves against it, both militarily, and as this hearing is going to show, electronically in terms of protecting the power grid that provides electricity for our great Nation.

I think we have a lot to learn in this area because the whole idea of a cyber attack is something that is, quite frankly, somewhat foreign to most of us, myself included. We have some feeling for the physical attacks which we have seen against our Nation time after time. But this is a new type of attack.

What are the vulnerabilities? Is our electricity grid adequately protected? Will a one-time cyber reliability rule solve the problem, or do we have to have redundant systems and change those over time to upgrade against the continually changing threat? What are the consequences of a cyber attack if successful? Is it a matter of losing power in a certain region for a few hours? Is it a matter of destroying critical equipment, or is it a matter of losing power all over our great Nation for long periods of time? We simply don't know.

Should the government write cybersecurity standards in this case, the Federal Energy Regulatory Commission, because under current law, the North American Electric Reliability Corporation, or Council, is simply too slow? If so, where should we draw the line? Do we address the bulk power system? What about military installations? What about local distribution systems? What about rural electric co-ops within single state boundaries? How do we do those?

What about Canada and Mexico? What are their views giving the FERC authority for the first time to coordinate and regulate with these nations that aren't within our own boundaries? Can we enforce such regulations if we agree that they are in the interest of these three nations? What about the views of the Defense Department and the National Security Council? What do they think about giving FERC the authority that we are thinking about giving them?

Whatever we do in this subcommittee and next week in the full committee, this is certainly an issue that needs to be addressed, and I want to commend you, Mr. Chairman, for addressing it. I want to welcome our witnesses today. The distinguished subcommittee chairman of the Homeland Security Committee, the distinguished chairman of the Federal Energy Regulatory Committee Commission and the other witnesses.

I do want to say one thing, Mr. Chairman, before I yield back. It was my understanding that Mr. Kelliher was going to be on a panel by himself. I see that you have him listed on a panel with non-elected officials. I think that is unacceptable. If I had known that was the way it was going to be, I would have objected strenuously. So I hope that before you actually begin the hearing, you will give a presidential appointee the courtesy that we have always given other appointees, and that is to testify by himself or herself.

Mr. BOUCHER. Would the gentleman yield?

Mr. BARTON. Sure.

Mr. BOUCHER. I thank the gentleman for making those remarks and comments, and would advise him that in the interest of time, Mr. Kelliher has graciously agreed to be a part of the second panel; although, he will be the first witness on that panel. Given the fact that we had the memorial today at the Pentagon this morning, and there is a subsequent one involving the House of Representatives at 11:45 and the urgency of addressing this issue, this was the only morning we could do it.

And given that urgency, Mr. Kelliher has graciously agreed to help us expedite our proceedings by allowing us just to have one panel of witnesses following the statement that Mr. Langevin will make. And I thank him for that and——

Mr. BARTON. It is not——

Mr. BOUCHER. Otherwise, I can assure the gentleman that we would have done as he suggests.

Mr. BARTON. Well, I appreciate the gentleman's—the chairman's explanation. With that, Mr. Chairman, I yield back.

Mr. BOUCHER. Thank you very much, Mr. Barton. The gentleman from Louisiana, Mr. Melancon, is recognized for 3 minutes. Mr. Melancon waives his opening statement and will have 3 minutes added to his questioning time for the second panel of witnesses. The gentleman from Michigan, Mr. Rogers, is recognized for 3 minutes.

OPENING STATEMENT OF HON. MIKE ROGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. ROGERS. Thank you, Mr. Chairman. I happen to serve on the Intelligence Committee with Mr. Langevin, and so I am at least glad that he is paying attention to this because I think he will bring a good perspective from that side of the House. And I am not sure sometimes if it is a benefit or a hindrance being on that committee.

And today, I am not sure either because I worry a little bit about the speed at which we are working here. We watched through the creation of the Director of National Intelligence that we were trying to coordinate our activities and our resources. And in a bipartisan way in this Congress we said slow down.

The exponential growth was not necessarily serving the interests of national security. And our cyber infrastructure goes well beyond the grid. The grid is an incredibly important part of that protection and security apparatus, but it is a part of that.

And we have lots of talent and lots of resources spread across the 16 intelligence agencies and Department of Defense, who have spent some serious amount of time and accumulated intellectual capital necessary to defeat what we know is a growing threat. And it is from terrorist organizations. It is from extortionists. It is joy riders on the superhighway, if you will, and it is certainly and very worrisome more aggressive by nation-states. And we see all of that activity growing exponentially. So the threat is very, very real.

But my concern is we are doing a ready, shoot, aim approach to how we are going to solve this problem because what we are going to do, even if you give authorities, with that will go people and resources. And then they have to go back and try to find integration with the very organizations I just mentioned before.

I am not sure that that is the right way to get where we want to go, and I want to commend all of you for working on this. I think it is a very, very important issue, and it is a serious issue. But I don't think creating a separate group through separate authorization is likely to get where we want to go in a timely manner.

We have resources. We have coordination efforts already that we are trying to work through, and I think Mr. Langevin is certainly aware of those. And I am not sure this helps it. Matter of fact, in some cases, I think it might actually hinder it. So I hope that we take our time and slow down a little bit. I think it is great that we highlight the problem, but the fact that we don't have representation from Department of Defense, from the National Security Council, from the intelligence community, quite frankly from the DNI. I think the DNI should—these are exactly the issues of which the director of national intelligence by this Congress was designated to help us move through some of these integrated policy issues where there is a cross spectrum of resources.

So again I hope the hearing is for informational purposes. I would not be in a hurry, Mr. Chairman, to pass a bill and move it through the House without the full cooperation and coordination of those resources. I think it would be critical to the end here that we do this correctly.

Mr. BOUCHER. Would the gentleman yield?

Mr. ROGERS. Absolutely. Yes, sir.

Mr. BOUCHER. I thank the gentleman for those remarks, and I agree with the gentleman completely. There is a great sense of urgency that we address this need, as our witnesses will tell us this morning. On a bipartisan basis, we have constructed a discussion draft which addresses the core concerns that have been brought to us. There are some open issues which I have identified. They will be discussed here as well this morning.

We invited the Department of Defense to send a witness to address the subcommittee this morning, and the Department of Defense declined to do that. I can tell the gentleman that we do intend to have a classified briefing for the—an opportunity offered to members for a classified briefing next week, and the Central Intelligence Agency. And the director of Central Intelligence will be a part of that briefing. And so the gentleman's request will be honored.

I can tell him also that we intend to go through regular order in processing this legislation. Assuming that we are in a position to resolve the outstanding issues, and I very much hope that we will be, we would like to move to a markup next week. That would be after the classified briefing takes place.

If the issues are resolved to the satisfaction of members, I see no reason why we shouldn't do that, given the urgency that exists. And then hopefully we can move to the full committee rapidly after that and then to the House floor. But I respect what the gentleman is saying, and he has expressed my view as well that we need to be very careful as we construct this measure. And we certainly intend to be.

Mr. UPTON. And if the gentleman will just yield. I have had some discussions with the chairman, Chairman Boucher, on this issue, and I agree that we ought to have regular order here. There are

a number of witnesses that are not on the list that ought to be here. Just looking at the brief presentation that CNN made on the air I want to say it was last year, there are a number of folks, Homeland Security agency and others, that really ought to be represented.

We need to do this right. It is critical. I don't have the luxury as you have, serving on the Intelligence Committee, Mr. Langevin and others. And as we are prepared to make sure that this is our level best, we have to have that input which is one of the reasons why the chairman and I thought it would be wise to have a classified briefing at the earliest moment which is, since we don't have votes tomorrow until Monday afternoon, Tuesday morning was the earliest time that we could do that to afford all members on both sides of the aisle to be able to ask questions in a private way.

It will lend us a better understanding of the way that we should proceed and do it in the right course.

Mr. ROGERS. And I commend you for having that classified briefing. I think hopefully that will give us a different look at it, and I would understand why DOD might have a hard time here. Some of the things that our communities are working on are very, very sensitive.

And because of the aggressive state of nation-states involved in cyber espionage and cyber terrorism, I can understand why they might have some reluctance to come here and not be able to answer questions. It puts it in an awkward place. So I hope that we take the time to see with this classified briefing.

And I think it might help us all understand how yes, it is important, but it is more important that we do it right than we do something.

Mr. UPTON. That is right. And your attendance there will help all of us in terms of what you have been able to go through because of your experience on the Intelligence Committee.

Mr. BOUCHER. I thank the gentleman for his contributions this morning. The gentleman from Oregon, Mr. Walden, is recognized for 3 minutes.

Mr. WALDEN. Mr. Chairman, I will waive an opening statement. Thank you, sir.

Mr. BOUCHER. Thank you very much, Mr. Walden. We now welcome our first witness this morning, the Honorable Jim Langevin from Rhode Island, and we appreciate very much your attendance here. Mr. Langevin is the chairman of the Subcommittee on Emerging Threat, Cybersecurity, and Science and Technology of the Committee on Homeland Security, and I know from my discussions with him, has been actively involved in examining the question of cybersecurity for his tenure of chairman of that subcommittee. And he has much useful information he can share with us this morning.

So, Jim, we welcome you, and your prepared statement will be made a part of the record. And we would welcome your oral remarks.

STATEMENT OF JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY, COMMITTEE ON HOMELAND SECURITY

Mr. LANGEVIN. Thank you, Mr. Chairman, and good morning. I would like to thank Chairman Boucher for his invitation to testify on this critical——

Mr. BOUCHER. If you could move that microphone a little bit closer and be sure it is on, that would help us in hearing you. Thank you.

Mr. LANGEVIN. Is that better?

Mr. BOUCHER. That is better.

Mr. LANGEVIN. Very good. I want to thank Chairman Boucher for his invitation to testify on this critical issue of national security. I very much appreciate the chairman's interest and that of Ranking Member Upton, and your interest in cybersecurity relates to the electric grid. And I commend both these gentlemen, the full committee, and its staff for their efforts in this area.

I would also like to thank Chairman Thompson of the Homeland Security Committee for his proactive leadership on these issues as well.

Mr. Chairman, as you mentioned, I chair the Emerging Threat, Cybersecurity, and Science and Technology Subcommittee for the Homeland Security Committee where I have conducted eight hearings and dozens of investigations on cybersecurity issues during the 110th Congress. I am also a member of the House Permanent Subcommittee on Intelligence, and I co-chair the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency.

Each of these positions has afforded me the opportunity to examine the issues that are before this committee today. Now, I want to clearly state that I believe America is disturbingly vulnerable to a cyber attack against the electric grid that could cause significant consequences to our Nation's critical infrastructure.

Virtually every expert I have consulted shares this assessment. Though I cannot provide classified details at this hearing, I hope that my testimony will support this assertion, encourage you to act on this legislation.

The effective functioning of the bulk power system is highly dependent on control systems, computer-based systems used to monitor and control sensitive processes and physical functions. Once largely closed to the outside world, control systems are increasingly connected to open networks, and the risks to these systems is steadily increasing.

Consider what has happened in the last 5 years. Criminal extortion schemes have exploited control systems for economic gain. Numerous disruptions from the Davis-Besse Power Plant incident in 2003 to the Northeast blackout, to the Browns Ferry Nuclear Power Plant failure in 2006 were caused by unintentional cyber incidents.

Furthermore, the U.S. has evidence that Al Qaeda is interested in the vulnerabilities of our public and private utilities. Additionally, nation-state adversaries have publicly stated that attacking our domestic critical infrastructure, including the civilian electric

grids, will be part of their war plans in an engagement with the United States.

Clearly intentional and unintentional control system failures on the BPS can have a potentially devastating impact on the economy, public health, and national security of the United States. Now, for a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, and water systems presents a terrifying scenario. These incidents would also severely impact our war-fighting capability as recognized by the Defense Science Board.

In the interest of national security, we must ensure effective and reliable energy flows to America's critical infrastructure facilities. With this in mind, my subcommittee initiated a review of the Federal Government's efforts and ability to ensure the security of the BPS from cyber attack.

We became particularly concerned about the private sector's efforts to mitigate a vulnerability known as Aurora, which the chairman mentioned in his opening remarks, which if exploited, could result in catastrophic losses of power for long periods of time. I was convinced of the seriousness of this vulnerability and began doing all I could to ensure that we were fixing it.

In June 2007, the Electric Sector Information Sharing and Analysis Center introduced a voluntary mitigation document to the industry. During my review of the electric sector mitigation efforts, however, it became evident that mitigation was highly inconsistent. I was surprised and disturbed to see how dismissive many of the companies were of this vulnerability, particularly given the significant technical evidence backing up the test.

Even worse, NERC, the private sector reliability organization, seemed uninterested in determining the extent of industry compliance. NERC provided false, confusing, or misleading testimony to my subcommittee during our investigation. Now, NERC has since realized their mistakes, corrected their testimony, and began demonstrating the leadership that we expect. Nevertheless, I am still worried about the electric sector's approach towards timely mitigation of cybersecurity vulnerabilities.

Now, in light of this failure of initiative throughout the electric sector, my subcommittee made a formal request of FERC to investigate the extent to which owners and operators were implementing the Aurora mitigation efforts. Thankfully, FERC has demonstrated great initiative, and I want to take this opportunity to publicly thank Chairman Kelliher and his staff for their efforts.

FERC's initial observations suggest that while no company completely ignored the advisory, there were varying degrees of compliance. At this time, the subcommittee also requested that FERC assess its ability to respond to an imminent cyber attack under the current legal authorities contained in section 215 of the Federal Power Act. In testimony before the subcommittee on May 21, Chairman Kelliher concluded that additional authorities are necessary to adequately protect the BPS, and I fully support the chairman's conclusion.

In the interest of national security, a statutory mechanism is necessary to protect the grid against cybersecurity threats. I congratulate the subcommittee for its legislative initiative, and I have several comments on the draft legislation that are before us.

First, emergency standards should become enforceable upon a finding by a national security or intelligence agency. I fear that additional executive determinations would create unnecessary delays in the protections of the BPS.

Second, FERC should be authorized to act if either one, a malicious act is likely to occur, or two, there is a substantial possibility of disruption to the grid due to such an act. Specific threat information on this subject is difficult to come by, and it would be very hard to put together likelihood and consequence. We must not limit the ability of our federal agencies to act.

Finally, I am concerned that the current legislation does not cover assets that are outside the definition of the bulk power system, which, if left unprotected, will keep our Nation vulnerable. As the committee is aware, and as the chairman had referred to, the Federal Power Act leaves vulnerable Alaska, Hawaii, and many other—and many major cities like D.C. and New York and the Nation's critical infrastructures like our military installations because they don't fall under the definition of the BPS.

Generation, transmission, and distribution must be protected under this legislation, and I would ask the committee to consider an amendment that would allow FERC to address cyber threats against all of these areas.

Now, in closing, on this day when we vow to be vigilant in protecting the country against threats of all kinds, let nobody accuse us of having a September 10 mindset when it comes to cybersecurity.

With that, I want to thank you, Mr. Chairman, for allowing me the opportunity to testify today, and I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Langevin follows:]

Summary Statement from James R. Langevin
Chairman, Emerging Threats, Cybersecurity,
Science and Technology Subcommittee
U.S. House of Representatives Committee on Homeland Security

Hearing before the House Committee on Energy and Commerce
Subcommittee on Energy and Air Quality
September 11, 2008

- There is significant risk of cyber attack against the Bulk Power System ("BPS").
- Intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the United States.
- The Homeland Security Committee has conducted extensive oversight investigations and held two hearings on cybersecurity and the electric grid during the 110th Congress.
- The Subcommittee on Emerging Threats, Cybersecurity, Science and Technology Technology initiated a review of the Federal government's effort and ability to ensure the security of the BPS from cyber attack, focusing particularly on a vulnerability to the BPS discovered by engineers at the Idaho National Laboratory.
- The Subcommittee learned that owners and operators of the BPS were not mitigating this vulnerability to the expectations of Congress and the Federal Energy Regulatory Commission ("FERC").
- The Subcommittee requested that FERC assess its ability to respond to an imminent cyber attack under the current legal authorities contained in Section 215 of the Federal Power Act ("FPA").
- Chairman Kelliher concluded during a Subcommittee hearing on May 21, 2008 that additional authorities are necessary to adequately protect the BPS against cyber attack.
- I fully support the Chairman's conclusion. In the interest of national security, a statutory mechanism is necessary to protect the grid against cyber security threats.
- I have three comments to the legislation: 1) emergency standards should become enforceable upon a finding by a national security or intelligence agency; 2) "cybersecurity threats" should mean "likelihood" <u>or</u> "substantial possibility of disruption"; 3) legislation should include protections for Alaska, Hawaii, territories, and distribution facilities.

Statement of James R. Langevin
Chairman, Emerging Threats, Cybersecurity,
Science and Technology Subcommittee
U.S. House of Representatives Committee on Homeland Security

Hearing before the House Committee on Energy and Commerce
Subcommittee on Energy and Air Quality
September 11, 2008

I. Introduction and Overview

Good morning. I'd like to begin by thanking Chairman Boucher for his invitation to allow me to testify on this critical issue of national security. I very much appreciate the Chairman's interest in the subject of cybersecurity as it relates to the electric grid, and I commend him, the full Committee, and the staff for their efforts in this area. I would also like to thank Chairman Thompson of the Homeland Security Committee for his proactive leadership on cybersecurity and other issues of national security.

I serve as Chairman of the Emerging Threats, Cybersecurity, Science and Technology Subcommittee for the Homeland Security Committee, where I have held eight hearings and conducted dozens of investigations on cybersecurity issues during the 110th Congress. During this time, the Committee on Homeland Security conducted a review into the efforts of owners and operators of the bulk power system ("BPS") to secure their information networks. I want to clearly state that I believe America is disturbingly vulnerable to a cyber attack against the electric grid that could cause significant consequences to our nation's critical infrastructure. Virtually every expert that I've discussed these matters with – across government and throughout the private sector – shares this assessment. Though I cannot provide classified details at this hearing, I hope that the following sections will support this assertion.

In testimony before the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology on May 21, 2008, Chairman Joseph Kelliher of the Federal Energy Regulatory Commission ("the Commission") stated that his agency is in need of

additional legal authorities to adequately protect the BPS against cyber attack. I fully support the Chairman's request for these authorities. However, I am concerned that the current legislation does not cover assets that are outside the scope of the Federal Power Act definition of BPS, which, if left unprotected, will keep our nation vulnerable. I respectfully submit the following comments for the Committee's consideration.

II. Background: Threats and Vulnerabilities to the BPS

The BPS of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability, serving over 300 million people.[1] The effective functioning of this infrastructure is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks."[2]

The risk to these systems is steadily increasing. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the BPS, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[3] Since the release of that study, numerous unintentional cyber incidents – from the Davis-Besse power plant incident in 2003, to the Northeast

[1] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.
[2] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.
[3] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.

blackout, to the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted. Malicious actors also pose a significant risk to this infrastructure. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states, domestic criminals and hackers, and disgruntled employees working within an organization.[4]

There are numerous public examples of threats and vulnerabilities that have had a negative and dangerous impact on electric systems. The potential consequences of an attack on control systems vary widely from the introduction of raw sewage into potable water systems[5] to the catastrophic failure of critical electrical generators due to the change of a single line of code in a critical system.[6] For example:

- Computers at an inactive nuclear power plant in Ohio were infected by the Slammer worm in January 2003.[7]
- Multiple criminal extortion schemes have exploited the use of control systems for economic gain.[8]
- There is evidence that al Qaeda is interested in the vulnerabilities of the U.S. public and private utilities.
- The discovery in Afghanistan of a computer containing structural analysis programs for dams, combined with an increase in Web traffic relating to SCADA systems, prompted the National Infrastructure Protection Center ("NIPC") to issue a warning information bulletin.[9]
- Nation state adversaries have suggested that attacking our domestic critical infrastructure will be part of their war plans in an engagement with the United States. In a book endorsed by top Chinese People's Liberation Army leadership called "Unrestricted Warfare," two colonels describe using network attacks "to

[4] U.S. Government Accountability Office, Report to Congressional Requesters, *TVA Needs to Address Weaknesses in Control Systems and Networks* (April 2008), p. 8.
[5] U.S. Government Accountability Office, Report to Congressional Requesters, *Challenges and Efforts to Secure Control Systems* (2004) p. 17..
[6] Briefing by NCSD, INL to the Homeland Security Committee, March 15, 2007.
[7] Congressional Research Service "Critical Infrastructure: Control Systems and the Terrorist Threat," RL31534, p. 17.
[8] Infoworld, "Government cybersecurity gets an 'F,'" Sep. 11, 2006, available at http://www.infoworld.com/article/06/09/11/37NMmain_1.html.
[9] CRS Report RL31534, p. 7.

> disrupt the civilian electricity network, traffic dispatching network, financial transaction network, and telephone communications networks," causing social panic and undermining political leadership.

Clearly, intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the United States. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, and water systems presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.[10] This figure does not consider the negative societal or health ramifications that such an event would have on the American people.

An intentional or unintentional attack would also severely impact the ability of our war fighting capability. The Defense Science Board recently recognized the threat to critical Department of Defense ("DOD") military facilities that rely on the BPS. In a report titled "More Fight – Less Fuel" issued in February 2008, the Board concluded that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid and other critical national infrastructure."[11] The Board stated the grid "is highly vulnerable to prolonged outage from a variety of threats. This places critical mission assets at unacceptably high risk of extended disruption."[12] Furthermore, in the event of an attack on the BPS, the Board noted that the U.S. military cannot rely on on-site backup power generation:

> Although 99 percent of the electricity at U.S. military installations is from the commercial grid, backup power at installations is based on diesel generator sets with limited on-site fuel storage and not prioritized to critical tasks. As the reliability of the national grid has declined, the

[10] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.
[11] Report of the Defense Science Board Task Force on DOD Energy Strategy, *More Fight – Less Fuel*, February 2008, available at http://www.acq.osd.mil/dsb/reports/2008-02-ESTF.pdf.
[12] Id., p. 53.

> adequacy of backup power has become an issue. For both war fighting-related activity and the new Homeland defense mission, backup power is inadequate in terms of size, duration and reliability.[13]

The Board concluded that the DOD's approach to providing power to installations is based on assumptions that commercial power is highly reliable, subject to infrequent and short term outages, and backup can meet demands. Unfortunately, DOD's assumptions about commercial power and other critical infrastructure reliability are no longer valid and DOD must take a more rigorous risk-based approach to assuring adequate power to its critical missions. In the interest of national and homeland security, we must ensure effective and reliable energy flows to America's critical infrastructure facilities.

III. Homeland Security Committee Oversight: Aurora Investigation

With these issues in mind, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology initiated a review of the Federal government's effort and ability to ensure the security of the BPS from cyber attack. In October 2007, the Subcommittee held a hearing on the cyber threat to control systems, focusing particularly on a vulnerability to the BPS discovered by engineers at the Idaho National Laboratory. The vulnerability – known as "Aurora" – could enable a targeted attack on infrastructure connected to the electric grid, potentially destroying these machines and resulting in catastrophic losses of power for long periods of time. After engineers demonstrated a successful test of the vulnerability, the Department of Homeland Security ("DHS"), the Nuclear Regulatory Commission ("NRC") and the Commission began leading an effort to reach out to the private sector to mitigate the vulnerability.

Under the framework of the Partnership for Critical Infrastructure Security,[14] DHS began its outreach efforts with the Electric and Nuclear sectors, which each identified a technical team and a set of subject matter experts to develop a mitigation

[13] Id.

[14] The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

strategy.[15] These two sectors began implementing the mitigations in varying degrees. On June 20, 2007, the Nuclear Sector issued a requirement for all members of their sector to implement short, medium, and long term mitigations for the vulnerability. On June 21, 2007, the Electric Sector (through the Electric Sector Information Sharing and Analysis Center, ES-ISAC) sent an advisory to its members with recommendations that they take similar action.

During the Subcommittee's hearing in October, it became evident that the Nuclear Sector was well on its way toward implementing the mitigations; however, the extent to which Electric Sector companies were following the recommendations of the advisory was not clear. The difference in each sector's implementation stemmed from the cybersecurity regulatory requirements. In October 2007, the Commission had not yet adopted the Critical Infrastructure Protection reliability standards proposed by the North American Electric Reliability Corporation ("NERC"), which addressed cybersecurity requirements for the Electric Sector. Therefore, while the NRC could issue specific requirements for its owners and operators, the Electric Sector was unable to make similar demands.[16] Members of the Committee expressed concern during the hearing that these mitigation measures were not being fully implemented in the Electric Sector.

These concerns were justified. Though NERC testified during the hearing that it sent a survey to industry members to determine compliance with the advisory and received a response from approximately 75 percent of the transmission grid that mitigations had been implemented or were in the process of being implemented,[17] the

[15] The Department held briefings at the FOUO level rather than classifying the information to the Secret level. The Department's justification for this was the importance of having the private sector aware and involved with mitigation of the vulnerability.

[16] Several things have changed since the Subcommittee hearing. On January 17, 2008, the Commission approved eight mandatory critical infrastructure protection reliability standards to protect the bulk power system against potential disruptions from cyber security breaches. These standards were developed by NERC, the private sector organization designated by the Commission as the electric reliability organization (ERO). These standards are currently in effect, though the industry has until approximately 2010 before they have to demonstrate "auditable compliance" with the standards. See NERC Revised Implementation Plan for Cybersecurity Standards.

[17] U.S. Congress, House Committee on Homeland Security, Hearing on "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid," *testimony of David Whiteley,* 110th Cong., 1st sess., 17 Oct. 2007.

Committee later learned that the survey was not sent until October 19, 2007 – two days after the hearing.[18] Later, NERC staff suggested that they received information about the industry's mitigation efforts during a Critical Infrastructure Protection Committee meeting in St. Louis in September 2007. However, when the Committee asked participants about that meeting, none of the attendees were able to confirm that they discussed their mitigation efforts with NERC.

In light of these discrepancies, in mid-October 2007, the Subcommittee, on a bipartisan basis, requested that Chairman Kelliher investigate the extent to which Electric Sector owners and operators implemented the mitigation efforts from the original Aurora advisory. Chairman Kelliher had expected to be able to draw upon results from NERC's October 19 industry survey; however, he determined that the survey lacked sufficient details of the mitigation efforts that would have provided the Commission with the certainty that the vulnerability had been addressed. For example, NERC's survey did not provide information about what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken – and, if certain actions were not being taken, why not. The Commission determined that it would have to undertake its own independent survey in order to obtain the information requested by the Homeland Security Committee.

The Commission is currently in the process of working with industry groups to informally gather information, on a voluntary basis, regarding the status of compliance with NERC's Aurora advisory. Initial observations suggest that while no company interviewed ignored the advisory, there was a broad range of compliance based on individual interpretations of the threat and the application of the recommended mitigation measures. In fact, all of the utilities interviewed requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, the Commission has determined that although progress has been made by every entity that it interviewed much work remains to be done.

[18] Electric Sector ISAC (ESISAC) Advisory Follow-up Survey, Oct. 19, 2007.

I was deeply disturbed that a thoroughly tested vulnerability which could cause catastrophic damage to the BPS was not being mitigated by the private sector. I began searching for other means by which we – the U.S. Congress – could ensure that the BPS (and the American populace that relies on its effective function) is being protected against these vulnerabilities. Therefore, contemporaneous with its request for a Commission-led investigation, my Subcommittee also requested that the Commission assess its ability to respond to an imminent cyber attack under the current legal authorities contained in Section 215 of the Federal Power Act ("FPA"). I was concerned that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the promulgated standards,[19] but also the authority to issue orders to owners and operators in the event of an imminent exploitation of a BPS asset.

In testimony before the Subcommittee on May 21, 2008, Chairman Kelliher agreed with my preliminary assessment, and concluded that additional authorities are necessary to adequately protect the BPS against cyber attack. The Chairman noted that while Section 215 may adequately protect the BPS against most reliability threats, the cybersecurity threat is different:

> [Cybersecurity] is a national security threat that may be posed by foreign nations, or others intent on undermining the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Given the national security dimension to the cyber security threat, there may be a

[19] The Homeland Security Committee has also argued that the NERC reliability standards are inadequate for protecting critical national infrastructure. For instance, telecommunications equipment is excluded from the standard's definition "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations. Ironically, some of these assets that could be exploited in an attack using the Aurora vulnerability are not considered "critical cyber assets." This means that if the Aurora vulnerability was discovered again tomorrow, NERC could not issue a "required action" to owners and operators under its jurisdiction because the "assets" affected by the Aurora vulnerability are not currently covered by CIP standards.

need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action.[20]

IV. Comments on the Draft Legislation

I fully support the Chairman's conclusion. In the interest of national security, a statutory mechanism is necessary to protect the grid against cybersecurity threats. I believe that the FPA should be amended to grant the Commission emergency authority to order temporary interim cybersecurity or other emergency standards when necessary to protect against a national security threat to the reliability of the BPS. I have several comments on the draft legislation.

First, I believe that emergency standards should become enforceable upon a finding by a national security or intelligence agency in consultation or coordination with FERC that there is a national security threat to the BPS. I fear that the Presidential/Secretarial determinations, as currently provided for in the draft legislation, could create unnecessary delays in the protection of the BPS. An event in cyberspace may happen in seconds, but determining to authorize authorities for a response could take hours or days -- time that we simply cannot afford to waste.

Second, I believe that the President or the Department of Energy (or intelligence authorities, as suggested above) should be authorized to direct FERC action if either (1) a malicious act is likely to occur or (2) there is a substantial possibility of disruption to the grid due to such an act. Thus, I would recommend that the definition read "Cybersecurity threat means that there is credible information or evidence of (1) the likelihood of a

[20] U.S. Congress, House Committee on Homeland Security, Hearing on "Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid," *testimony of Joseph Kelliher*, 110th Cong., 2nd sess., 21 May 2008. Chairman Kelliher noted that "cyber vulnerabilities can require swift remedial action to protect the Nation's bulk power system," and that the standards development process can be "relatively slow." Furthermore, even though the Commission has an "Urgent Action" process, this can take one to three months to implement.

malicious act that could disrupt the operation of those programmable electronic devices and communications networks…that are essential to the reliable operation of the bulk power system; or (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act."

Finally, the scope the bill is limited to facilities that comprise the BPS as defined in section 215 of the FPA. I feel compelled to discuss what I believe is a conceptual error in the FPA's definition of the BPS. The BPS is defined as the generation plants, the high voltage transmission system, and associated equipment, and does not normally include the distribution substations and lower voltage networks that distribute electricity to customers in a particular city or region. Alaska and Hawaii are specifically excluded from reliability regulations. In practice, many major cities and population centers are also excluded. This limitation leaves our nation vulnerable.

In January 2008, FERC approved the reliability standards developed by NERC to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. By definition and design, the BPS CIP Standards do not recognize the importance of continuity of electric power to chemical plants, banks, refineries, hospitals, water systems, and military installations, in and of themselves. Where they are located or their importance to society is not a factor in the determination of what parts of the greater U.S. electric system should be protected. This means that <u>any</u> Critical Infrastructure Protection ("CIP") Standards – including those recently approved by FERC – will focus on reliability of the BPS exclusively, and not on public health and safety or even economic stability from a "homeland security" perspective.

Before the terrorist attacks against our country on September 11, 2001, a single-minded focus on BPS reliability against serendipitous hazards and accidents may have been appropriate; but with the specter of terrorist or nation-state-directed force against the

U.S. public at large, preoccupation with the BPS as a whole falls short of the mark. For example, the reliable operability of a small substation powering a major oil or gas pipeline in a remote region is not important to the stability of the BPS grid, but an extended failure of that asset could very well have profound adverse consequences for the stability, and even the viability, of the U.S. economy or national security. I believe those small substations should be covered under Federal regulation.[21]

If the correct objective of the national electric power system is to generate, transmit, and reliably deliver electricity all the way out to the eventual end user – the public – then there are more links in this mission-chain than just the BPS, and the CIP Standards fall short of the mark. To enhance the national security, I believe this is an issue that the Committee on Energy and Commerce must re-examine.

For purposes of this legislation, I would ask the Members to consider an amendment that would allow FERC to direct measures or actions aimed at protecting Alaska, Hawaii, and the territories from reliability threats, as well as distribution facilities. This would cover most or all of the grid facilities in large cities such as New York and Washington, D.C., and the nation's critical military installations that are connected to the BPS. In passing this amended legislation, this Committee would truly be protecting the national electric system.

V. Conclusion

Thank you for allowing me the opportunity to speak to you today on such an important matter facing our nation. The Homeland Security Committee will continue to remain diligent in investigating cybersecurity issues across the Federal government and

[21] Note that the BPS Transmission grid in the area hardest hit by Hurricane Katrina was restored within six days following the storm, but that did not help get municipal water department pumps back up and running because the Distribution systems were still off-line. The public in many hurricane-affected areas did not have running water for a considerable period of time. A hacker incursion resulting in disability of a Distribution control system(s), and/or key assets thereby managed, can be a BPS-independent event that still results in, by example, the pumps of an urban water system being disabled with the same adverse end result for the public. In this specific example, reliable delivery of power to the water infrastructure is also a health and safety issue, not just an inconvenience for the public.

throughout the national critical infrastructure. I look forward to working with the Committee on Energy and Commerce on these and other national security issues in the future.

Mr. BOUCHER. Thank you very much, Mr. Langevin. We appreciate that testimony, and your comments this morning will prove very helpful to us as we proceed with our work. I do not have questions of you, at least not at this time. We may consult you as we proceed with further steps in this process, but I do not have questions of you at this moment.

I would ask if there are other members of the panel who would care to pose questions to Mr. Langevin. Mr. Upton seeks recognition.

Mr. UPTON. I just have one. And, Jim, we appreciate your testimony and your work on this for sure. You indicated in your statement that you feared that the presidential secretarial determination as currently provided in the draft legislation would create an unnecessary delay in the protection of the BPS, but you have to have a chain of command.

And one of the issues that may be raised is FERC is certainly the appropriate agency overseeing the grid and all of that, but shouldn't you have someone at the White House or someone at the Pentagon, someone, perhaps the Secretary of Energy, someone with direct—not that our good friend Joe doesn't have access to folks like that.

But shouldn't you have some White House command similar to what happened on 9/11 when the FAA ruled, because of Secretary Menetta, that all the planes were going to stop wherever they were. That came in direct consultation with the White House, and, bingo, it happened. Shouldn't you have that type of chain of control—chain of command as part of the legislation which seems to be one of the criticisms that you might have here? Am I misreading what your comments were?

Mr. LANGEVIN. That is true, but certainly the Secretary of Homeland Security can be clearly a national emergency——

Mr. UPTON. Yes, that would be appropriate too.

Mr. LANGEVIN [continuing]. Along these lines. But we have to understand that in this day and age of cybersecurity, cyber attacks, it is one thing if we had days to go through the process of ultimately getting a presidential directive in place. But when we have actionable intelligence, these types of cyber attacks, cyber threats, could actually come in seconds or minutes or hours. And when we have direct actionable intelligence, there should be a rapid ability to respond.

And I am concerned about unnecessary delays. Even if this directive authority I am suggesting that FERC would be given would be temporary in nature until a more permanent solution can be addressed would be fine. But I think that we have to recognize in this day and age of cyber, things don't move in days or weeks. They move in seconds.

Mr. UPTON. I yield back.

Mr. BOUCHER. Thank you very much, Mr. Upton. Mr. Langevin, we appreciate your attendance here this morning, and we will move now to our second panel of witnesses.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. BOUCHER. We are pleased to welcome on the second panel the chairman of the Federal Energy Regulatory Commission, Mr. Joe Kelliher; Mr. Kevin Kolevar, the assistant secretary of the

United States Department of Energy; Mr. Rick Sergel, the president of the North American Reliability Corporation; Susan Kelly, vice-president and general counsel of the American Public Power Association; Steve Naumann, vice-president of the Exelon Corporation; and Barry Lawson, manager of power delivery for the National Rural Electric Cooperative Association.

We welcome each of our witnesses and thank you for your attendance this morning. And your prepared written statements will be made a part of our record. We would welcome your oral summaries and ask that in the interest of time, you try to keep your oral summaries to approximately 5 minutes.

We are going to operate slightly out of order this morning because both Mr. Kelliher and Mr. Kolevar have expressed a need to depart rather quickly in order to attend to some rather urgent outside business. And so we are going to take their opening statements first. We will ask questions of them, and then we will proceed to the opening statements and questions of the balance of our witnesses.

And so with that understanding, Mr. Kelliher, we will be happy to hear from you, and then Mr. Kolevar.

STATEMENT OF JOSEPH KELLIHER, CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

Mr. KELLIHER. Thank you, Mr. Boucher. Mr. Chairman, Mr. Upton, members of the subcommittee, I want to thank you for the invitation to testify here today, and I want to say it is good to be back before the subcommittee. I appreciate the opportunity to discuss the need to improve cybersecurity and to protect the reliability of the power grid against cyber attacks and other national security threats.

Three years ago, Congress made FERC responsible for protecting the reliability of the power grid by establishing and enforcing mandatory reliability standards. Congress specifically directed FERC to develop cybersecurity standards to protect the grid, and we have done so.

But I am here today to offer my conclusion that the tools you gave us 3 years ago are inadequate to the task and that FERC needs additional legal authority to adequately protect the grid from cyber attacks and other national security threats.

There has been much progress made on reliability over the past 3 years. FERC has certified an electric reliability organization. We have established mandatory reliability standards including cyber standards. We are working to improve those standards over time to raise the bar, and we have established a reliability enforcement regime.

But the grid remains vulnerable to a cyber attack through communication devices that could secure access control and remote operation of key components of our electricity system, such as large generating facilities, substations, transmission lines, and local distribution facilities. And that through remote operation, a cyber attack could damage or destroy generation in other facilities, and because an attack could damage or destroy facilities that could take weeks or longer to replace, the effects of a successful cyber attack could be much greater than a blackout.

In my view, an effective defense of the power grid from cyber attacks has three necessary elements. First, there is a need for timely and effective identification of cyber vulnerabilities. Second, there is a need to have an ability to require mandatory actions that mitigate those vulnerabilities on a timely basis, so action that is both rapid and mandatory. And third, the ability to maintain the confidentiality of information because current law is inadequate to mount such a defense.

FERC is not a national security or intelligence agency, and FERC is not in the best position to identify cyber threats. But the U.S. government has the ability to identify cyber threats in a timely and effective manner. FERC cooperates with agencies that are in that position, including the Department of Energy. However, there is no adequate means to take mandatory action in a timely manner under existing law.

Currently, there are two means to protect the power grid against cyber attacks. The 215 process established by Congress in the Energy Policy Act of 2005 and also NERC advisories. But in my view, neither is adequate to defend against cyber attacks. The 215 process produces reliability standards that are mandatory but untimely given the nature of cyber threats. And NERC advisories are timely or can be timely, but they are also voluntary. Both approaches fail to protect critical information.

FERC is using and will continue to use the process established by 215 of the Federal Power Act to set reliability standards including cyber standards. But the principal flaw of the 215 process is that it takes too long and does not allow for the protection of critical information. Under the normal 215 process, it typically takes years to develop new and modified reliability standards including cyber standards. Even reliability standards developed under the urgent action process can take months or longer.

Also FERC cannot modify a proposed standard. We can reject or remand or approve and direct changes that will occur over time, but if we reject a standard, it just simply reinitiates a process that could take months or years.

Why is there a need for timely action in this area? It is simply because the cyber threat is different from other reliability threats. The section 215 process was designed around a fundamentally different reliability challenge, namely vegetation management or tree growth, relay maintenance, grid control operations, and operator training. The reliability threat posed by trees and poor vegetation management is a passive threat, while the threat posed by cyber attacks is organized and much more active.

The nature of the cyber threat is different. It is a national security threat that may be posed by foreign countries or organized groups. A process designed to guard against poor vegetation management is poorly suited to meet national security threats. There is another limitation in that section 215 only authorizes FERC to ultimately establish standards and that some cyber threats or other national security threats may require action that are not standards.

NERC advisories also, I think, are an inadequate way to ensure or to protect cybersecurity. The principal virtue of a NERC advi-

sory is speed, but the principal flaw is that compliance with those advisories is voluntary. And there is a lack of confidentiality.

NERC issued an advisory last year in response to the Aurora cyber threat, and I commend NERC for acting quickly in response to that threat. As detailed in my written testimony, FERC has been reviewing the industry response to that advisory. I have to say the industry has made progress in response to the NERC advisory. I think cybersecurity is higher as a result, but our review indicates that the industry response has not mitigated the Aurora threat. And to some extent, that response is the predictable result of reliance on a voluntary advisory.

Now, confidentiality. I think it is also clear that an effective defense against cyber threats requires confidentiality. The standards development process under section 215 of the Federal Power Act typically imposes few or no restrictions on the dissemination of information related to development of new standards including cyber standards. The case of cyber vulnerabilities and public release of information related to cybersecurity could be very harmful, and that FERC currently has very limited authority to limit the public dissemination of information.

So in my view, I think there is a need for legislation. I think section 215 of the Federal Power Act is an adequate basis to address reliability threats other than national security threats, such as cyber attacks. And I, for that reason, do not believe that section 215 should be amended.

But I do believe there is a need for legislation that would grant FERC a separate authorization to, number one, immediately require measures to address known cyber vulnerabilities, such as related to Aurora, and two, require mandatory actions needed to protect the power grid from future national security threats on an interim basis after a finding by the President or the Secretary of Energy.

I think under this approach, it is clear FERC cannot act with respect to future cyber and other national security threats without such a finding by the President or the Secretary. So I think that it appropriately limits us and relies on the superior knowledge of the President and the Secretary with respect to national security threats.

It is also vital that a bill allow FERC to take action before a cyber attack and not only after the fact. It is critical that the threshold or trigger for a finding by the President or the Secretary not be so high as to be insurmountable, and I think the trigger in the proposed act discussion draft is appropriate.

There is also a need to address national security threats other than cyber, but I want to say I do support the staff discussion draft as is. It strikes the right balance, and I look forward to working with the subcommittee as you move towards markup.

And I do recognize the Department of Energy has a proposal that I think also should be considered as you move to markup in coming days.

In conclusion, you gave us the duty 3 years ago to protect reliability of the power grid, to establish and enforce reliability standards. We are exercising that duty, but we have come to the conclusion that we don't have the right tools to address the cyber threat.

And the reason is that the nature of the threat, the reliability threat to the grid is different than perhaps was anticipated 3½ years ago.

And so I do ask you to act and legislate, but until and unless you do that, FERC and NERC will use existing authorities. We will use the tools we have as best we can. And with that, I appreciate the opportunity to testify here today.

[The prepared statement of Mr. Kelliher follows:]

STATEMENT OF JOSEPH T. KELLIHER

SUMMARY

The Energy Policy Act of 2005 (EPAct 2005) authorized the Federal Energy Regulatory Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the bulk power system. These reliability standards are proposed to the Commission by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC), after an open and inclusive stakeholder process. The Commission cannot author the standards or make any modifications, and instead must either approve the proposed standards or remand them to NERC. FERC is well underway in implementing the new law, including now having in place an initial set of cyber security standards, for which full compliance is not required until 2010.

Section 215 is an adequate statutory foundation to protect the bulk power system against most reliability threats. However, the threat of cyber attacks or other intentional malicious acts against the electric grid is different. These are national security threats that may be posed by foreign nations or others intent on attacking the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance.

Damage from cyber attacks could be enormous. A coordinated attack could affect the electrical grid to a greater extent than the August 2003 blackout and cause much more extensive damage. Cyber attacks can physically damage the generating facilities and other equipment such that restoration of power takes weeks or longer, instead of a few hours or days. Widespread disruption of electric service can quickly undermine our government, military readiness and economy, and endanger the health and safety of millions of citizens. Thus, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect security-sensitive information from public disclosure.

The Commission's legal authority is inadequate for such action. This is true of both cyber and non-cyber threats that pose national security concerns. In the case of such threats to the electric system, the Commission does not have sufficient authority to timely protect the reliability of the system. Legislation should be enacted allowing the Commission to act promptly to protect against current cyber threats as well as future cyber or other national security threats.

TESTIMONY

INTRODUCTION AND SUMMARY

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to speak here today about cyber and other national security threats to our Nation's electrical grid, and the need for legislation allowing the Federal Energy Regulatory Commission (FERC or the Commission) to address those threats quickly and effectively. I appreciate the Subcommittee's attention to this critically important issue.

The Energy Policy Act of 2005 (EPAct 2005) gave the Commission certain responsibilities for overseeing the reliability of the bulk power system. The bulk power system is defined to include facilities and control systems necessary for operating an interconnected transmission network (or any portion thereof), and electric energy from generation facilities needed to maintain transmission system reliability. EPAct 2005 authorized the Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the bulk power system. Under this framework, reliability standards are developed and proposed to the Commission by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC) through an open and in-

clusive stakeholder process. The Commission cannot author the standards or make any modifications, and instead must either approve the proposed standards or remand them to NERC. The Commission is well underway in implementing the new law, including now having in place an initial set of cyber security standards with varying implementation dates. Much progress has been made in the past 3 years. However, more work needs to be done, both with respect to improving those cyber security standards and possibly adding new ones.

In my view, FERC does not have sufficient authority to guard against national security threats to reliability of the electric system. Legislation should be enacted allowing the Commission to act quickly to protect against current cyber threats as well as future cyber or other national security threats.

BACKGROUND

In EPAct 2005, the Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. section 215 requires the Commission to select an ERO that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter. The Commission also may initiate enforcement on its own motion.

The Commission has implemented section 215 diligently. Within 180 days of enactment, the Commission adopted rules governing the reliability program. In mid-2006, it approved NERC as the ERO. In March 2007, the Commission approved the first set of national mandatory and enforceable reliability standards. In April 2007, it approved eight regional delegation agreements to provide for development of new or modified standards and enforcement of approved standards by Regional Entities.

In exercising its new authority, the Commission has interacted extensively with NERC and the industry. The Commission also has coordinated with other federal agencies, such as the Department of Homeland Security, the Department of Energy, the Nuclear Regulatory Commission, and the Department of Defense. Also, the Commission has established regular communications with regulators from Canada and Mexico regarding reliability, since the North American bulk power system is an interconnected continental system subject to the laws of three nations.

CYBER SECURITY STANDARDS APPROVED UNDER SECTION 215

Section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk power system including "cybersecurity protection." section 215 defines reliable operation to mean operating the elements of the bulk power system within certain limits so instability, uncontrolled separation, or cascading failures will not occur "as a result of a sudden disturbance, including a cybersecurity incident." section 215 also defines a "cybersecurity incident" as a "malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

In August 2006, NERC submitted eight new cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009, and full compliance with the CIP standards would not be mandatory until 2010.

On January 18, 2008, the Commission issued a Final Rule approving the CIP Reliability Standards and concurrently directed NERC to develop modifications addressing specific concerns, such as the breadth of discretion left to utilities by the standards. For example, the standards state that utilities "should interpret and apply the reliability standard[s] using reasonable business judgment." Similarly, the standards at times require certain steps "where technically feasible," but this is defined as not requiring the utility "to replace any equipment in order to achieve compliance." Also, the standards would allow a utility at times not to take certain action if the utility documents its "acceptance of risk." To address this, the Final Rule directed NERC, among other things: (1) to develop modifications to remove the "reasonable business judgment" language and the "acceptance of risk" exceptions; and, (2) to develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception. A further example of this discretion involved the utility's ability to determine which of its facilities would be subject to the cyber security standards. For these requirements, the Commission addressed its concerns by requiring independent oversight of a utility's decisions by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the Commission. However, until such time as the standards are modified by the ERO through its stakeholder process, approved by the Commission, and implemented by industry, the discretion remains.

CURRENT PROCESS TO ADDRESS CYBER OR OTHER NATIONAL SECURITY THREATS TO THE BULK POWER SYSTEM

As an initial matter, it is important to recognize how mandatory reliability standards are established under section 215. Under section 215, reliability standards are developed by the ERO through an open, inclusive, and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability matter, including cyber security threats. However, the NERC process typically takes years to develop standards for the Commission's review. In fact, the cyber security standards approved by FERC took the industry approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for industry comment, are open, and are generally based on the procedures of the American National Standards Institute (ANSI). The NERC process is intended to develop consensus on both the need for the standard and on the substance of the proposed standard. Although inclusive, the process is relatively slow and cumbersome.

Key steps in the NERC process include: nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with approval requiring a quorum of votes by 75 percent of the ballot pool and affirmative votes by two-thirds of the weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; voting by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. NERC-approved standards are then submitted to the Commission for its review.

Generally, the procedures used by NERC are appropriate for developing and approving reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process is a strength of the process as it relates to most reliability standards. However, it can be an impediment when measures or actions need to be taken on a timely basis to effectively address threats to national security.

The procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action. If a significant vulnerability in the bulk power system is identified, procedures used so far for adoption of reliability standards take too long to implement effective corrective steps.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address a reliability vulnerability within 60 days. Also, NERC's rules of procedure include a provision for approval of urgent action standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat ex-

ists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice.

Even a reliability standard developed under the urgent action provisions would likely be too slow in certain circumstances. Faced with a cyber security or other national security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months or years. That would not be feasible under the urgent action process. In the meantime, the bulk power system would be left vulnerable to a known national security threat. Moreover, existing procedures, including the urgent action procedure, would widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, the proposed standard submitted to the Commission may not be sufficient to address the vulnerability. As noted above, when a proposed reliability standard is submitted to FERC for its review, whether submitted under the urgent action provisions or the usual process, the agency cannot modify such standard and must either approve or remand it. Since the Commission may not modify a proposed reliability standard under section 215, we would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

NERC'S "AURORA" ADVISORY AND SUBSEQUENT ACTIONS

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take voluntary action to guard against cyber or other vulnerabilities. That approach provides for quicker action, but any such advisory is not mandatory, and should be expected to produce inconsistent and potentially ineffective responses. That was our experience with the response to an advisory issued last year by NERC regarding an identified cyber security threat referred to as the "Aurora" threat. Reliance on voluntary measures to assure national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards cannot assure reliability of the bulk power system.

In response to the Aurora threat, NERC issued an advisory to certain generator owners, generator operators, transmission owners, and transmission operators. According to NERC, this advisory identified a number of short-term measures, mid-term measures and long-term measures designed to mitigate the cyber vulnerability. NERC asked the recipients to voluntarily implement the measures within specific time periods. NERC also sent a data request to industry members to determine compliance with the advisory. That data request was limited in scope, however, asking only that industry members indicate if their mitigation plans are "complete," "in progress," or "not performing."

The Commission determined that the information sought by NERC in the above data request was not sufficient for the Commission to discharge its duties under section 215 because it did not provide sufficient details about individual mitigation efforts for the Commission to be certain that the threat had been addressed. For example, it did not provide information such as what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken—and, if certain actions were not being taken, why not.

In October 2007, the Commission sought emergency processing by the Office of Management and Budget (OMB) of a proposed directive to require utilities to provide information immediately on their mitigation efforts. OMB posted the proposal for public comment in December 2007, and received several comments raising issues about the Commission's ability to protect sensitive information from public disclosure. The Commission ultimately asked OMB to hold the proposal in abeyance while Commission staff asked a sampling of generation and transmission entities to voluntarily discuss with staff their compliance with the Aurora advisory. In February, Commission staff began interviewing them. Commission staff has conducted 30 detailed interviews with a variety of electric utilities geographically dispersed across the contiguous 48 states, to assess the state of the industry's protection against remote access cyber vulnerabilities, including the Aurora vulnerability. Each interview typically lasted six to eight hours and utilities voluntarily participated. The utilities were well prepared with documents to explain their actions, and were very cooperative in responding to staff questions. Staff found a wide range of equipment, configurations and security features implemented by the utilities. Several observations can be made based on the interviews.

All of the companies selected by the Commission fully cooperated in the interviews. We learned that there was a broad range of compliance based on individual interpretations of the threat that affected the application of the recommended mitigation measures. In fact, all of the utilities interviewed by the Commission requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, FERC staff has determined that although progress has been made by almost every entity it interviewed, much work remains to be done and, in large part, the Aurora threat remains.

While NERC can issue an alert, as it did in response to the Aurora vulnerability, compliance with these alerts is voluntary and subject to the interpretation of the individual utilities. Because an alert is voluntary, it may tend to be general in nature, and lack specificity. Further, as Commission staff has found with the Aurora alert, such alerts can cause uncertainty about the specific strategies needed to mitigate the identified vulnerabilities and the assets to which they apply.

Damage from cyber attacks could be enormous. All of the electric system is potentially subject to cyber attack, including power plants, substations, transmission lines, and local distribution lines. A coordinated attack could affect the electrical grid to a greater extent than the August 2003 blackout and cause much more extensive damage. Cyber attacks can physically damage the generating facilities and other equipment such that restoration of power takes weeks or longer, instead of a few hours or days. The harm could extend not only to the economy and the health and welfare of our citizens, but even to the ability of our military forces to defend us, since many military installations rely on the bulk power system for their electricity. The cost of protecting against cyber attacks is difficult to estimate but, undoubtedly, is much less than the damages and disruptions that could be incurred if we do not protect against them.

The need for vigilance may increase as new technologies are added to the bulk power system. For example, "smart grid" technology may provide significant benefits in the use of electricity. These include the ability to manage not only energy sources, but also energy consumption, in the reliable operation of the Nation's electric grid. However, smart grid technology will also introduce many potential access points to the computer systems used by the electric industry to operate the electric grid. Security features must be an integral consideration. To some degree, this is similar to the banking industry allowing its customers to bank on line, but only with appropriate security protections in place. As the "smart grid" effort moves forward, steps will need to be taken to ensure that cyber security protections are in place prior to its implementation. The challenge will be to focus not only on general approaches but, importantly, on the details of specific technologies and the risks they may present.

KEY ELEMENTS OF NEEDED LEGISLATION

In my view, section 215 is an adequate statutory foundation to protect the bulk power system against most reliability threats. However, the threat of cyber attacks or other intentional malicious acts against the electric grid is different. These are national security threats that may be posed by foreign nations or others intent on attacking the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Though the nature of the threat is different, the consequences are identical. Widespread disruption of electric service can quickly undermine the U.S. government and economy and endanger the health and safety of millions of citizens. Given the national security dimension to this threat, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action. This is true of both cyber and non-cyber threats that pose national security concerns. In the case of such threats to the electric system, the Commission does not have sufficient authority to timely protect the reliability of the system.

I ask Congress to enact legislation, outside of section 215, containing the following major elements. The bill should direct the Commission to establish, after notice and opportunity for comment, interim reliability measures to protect against the threats identified in NERC's "Aurora" advisory and related remote access issues. These interim measures could later be replaced by reliability standards developed, approved and implemented under the section 215 process. The bill also should allow the Commission, upon directive by the President (directly or through the Secretary of Energy), to issue emergency orders directing actions necessary to protect the reliability

of the bulk power system against an imminent cyber security or other national security threat. Significantly, FERC could only act upon such a directive. This reflects the reality that the President and national security and intelligence agencies such as DOE are in a better position than the Commission to determine the nature of a national security threat, while the Commission has the expertise to develop appropriate interim reliability measures.

I emphasize that the latter authority should apply not only to cyber security threats but also to other national security threats. Intentional physical malicious acts (targeting, for example, critical substations and generating stations) can cause equal or greater destruction than cyber attacks and the Commission should have no less ability to address them when an emergency arises. This additional authority would not displace other means of protecting the grid, such as action by federal, state and local law enforcement and the National Guard, but the Commission has unique expertise regarding the reliability of the grid, the consequences of threats to it and the measures necessary to safeguard it. If particular circumstances cause both FERC and other governmental authorities to require action by utilities, FERC will coordinate with other authorities as appropriate.

The bill should allow measures or actions that might be imposed under this new authority to be replaced by standards developed under section 215 where applicable. For example, there may be circumstances in which use of the section 215 process would not be applicable, such as when targeted and/or temporary measures are necessary based on specific threat information. Also, the Commission should be allowed to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of this authority.

The bill also should address the following details. First, the bill should allow the Commission to take emergency action before a cyber or other national security incident has occurred, if there is a likelihood of a malicious act or a substantial possibility of disruption due to such an act. In order to protect the grid, it is vital that the Commission be authorized to act before a cyber attack. It is equally necessary that the threshold for a threat determination not be so high as to be insurmountable. Second, with respect to the Aurora and related cyber threats of which we are aware today, the Commission should be permitted and directed, after notice and comment, to require owners, users and operators of the bulk power system to take adequate measures to address those threats, and those measures should remain in effect until the measures are no longer necessary, for example, if replacement standards are approved and implemented under section 215. Third, with respect to other actions or measures the Commission might order to address future imminent threats to reliability, any time-triggered sunset provision applicable to emergency actions ordered by the Commission should allow an exception if the President (directly or through the Secretary of Energy) reaffirms the continuing nature of the threat. In the event that the action is determined to be no longer necessary or if the measures or actions ordered by the Commission are replaced by standards approved and implemented under section 215, the Commission should issue a "discontinuance" order.

Finally, Congress should be aware of the fact that if additional reliability authority is limited to the "bulk power system," as defined in the FPA, it would exclude protection against reliability threats and emergency actions involving Alaska and Hawaii and possibly the territories, including any federal installations located therein. The current interpretation of "bulk power system" also would exclude some transmission and all local distribution facilities, including virtually all of the grid facilities in large cities such as New York and Washington, D.C., thus precluding possible Commission action to mitigate imminent cyber or other national security threats to reliability that involve such facilities and major population areas.

CONCLUSION

The Commission's authority is not adequate to address urgent cyber or other national security threats. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Congress should address this risk now.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. BOUCHER. Thank you very much, Mr. Kelliher. Mr. Kolevar, we will be happy to hear from you.

STATEMENT OF KEVIN M. KOLEVAR, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEPARTMENT OF ENERGY

Mr. KOLEVAR. Thank you, Mr. Chairman, members of the committee, for the opportunity to testify before you today on this critically important matter. Let me just note at the beginning that, as you would expect, the chairman and I and our staff have discussed this issue on a number of occasions. I would like to associate myself with his remarks. I think that as we move forward, you will find broad agreement between the Department of Energy and the FERC.

This hearing addresses more than just a reliability concern. It addresses a national security concern. The Department of Energy and FERC and the electric sector must work cooperatively toward eliminating cyber vulnerabilities in control systems and preventing malicious cyber attacks on our electric infrastructure. Our Nation's electric power grid must be better protected. We must harden our power system.

The Department of Energy regularly discovers new vulnerabilities in the control systems employed by many utilities. This is not hyperbole. Let me assure you that cyber attacks against control systems have occurred, and they are becoming increasingly sophisticated.

The director of National Intelligence only underscored these concerns when he acknowledged earlier this year that cyber exploitation has not only grown more sophisticated but more targeted and more serious. Embedded processes and controllers in critical sectors are being targeted for exploitation and potentially for disruption or destruction with increasing frequency by a growing number of adversaries, not all of whom are in the pay of foreign governments.

According to one senior CIA analyst, some cyber intrusions in utilities have been followed by extortion demands. Cyber attacks have been used to disrupt power equipment in regions outside the United States, and in at least one case, a cyber-based disruption caused an outage that affected multiple cities.

Let me for a moment drill down on one point, and this actually speaks to Congressman Rogers's point. The following text is drawn from the intelligence community assisting us in preparation of this draft. For a nation-state to execute a coordinated attack across the Nation with certainty at a point in time chosen have geopolitical or military effect would require considerable planning and would require sustained access during an extensive preparation period to numerous points in the control systems that help operate the national grid.

Planning this type of attack would require extensive collection of information, expertise on both cyber and power systems, probably some type of extensive modeling to be sure of the effect, and then gaining and maintaining access to the actual target systems. Even maintaining reliable clandestine access requires resources and constant attention because system software and configurations change over time, and the adversary must be careful not to tip his hand with obvious activity.

Gaining initial access to particular systems may require the recruitment of insiders or conducting supply chain attacks, which might require months or years of preparation. Even gathering the necessary detailed information needed to identify targets and possible points of access may require some form of long-term clandestine operations.

As a matter of risk management, we need to make sure that we are not facilitating each of these critical steps for our adversaries by leaving ourselves open to collection of target information, open to easy access and reconnaissance or vulnerable by virtue of leaving systems misconfigured or unpatched.

The Departments of Energy and Homeland Security have been working with industry to increase awareness and to help them make sensible risk management choices. And, Mr. Chairman, I think this also speaks to the confidentiality requirements that the chairman mentioned.

To be clear, however, notwithstanding the many difficulties associated with the execution of a very serious cyber attack on the electric sector, the potential consequences are significant. For that reason, a limited role for the federal government is warranted if the Nation's energy infrastructure is to be protected.

The Department has been substantively engaged on this issue for some time. In 2003, DOE's Office of Energy Assurance, the predecessor program to the Office of Electricity Delivery and Energy Reliability, was designated to work directly with the energy owners and operators to protect energy infrastructures from all hazards and make them become more resilient.

DOE does this by selectively conducting vulnerability assessments and applying sound risk management practices at critical facilities, and we implement physical and cyber solutions to mitigate the risks based on the vulnerabilities we identify. To date, the department and its national laboratories have conducted test bed and onsite field assessments of 15 common control systems used widely across the energy sector.

These assessments have revealed vulnerabilities ranging in severity from minimal to high impact. With 17 testing facilities from five Department of Energy national laboratories, we are also constantly leveraging an extensive intelligence gathering network, proving methodologies, and highly skilled professionals from across the national security and intelligence communities, in particular DHS, to assess an interpret threat information.

Nevertheless, we need to do more and be thoughtful. The cyber threat to electric power systems is certainly among the most critical in our Nation's infrastructure. However, cyberspace has become critical to all of our other infrastructures as well with potential national security, economic, and safety concerns. As a Nation, we need to make sure that we are addressing risk management across all of our infrastructures in a holistic manner and that we not solve one problem only to create new problems or restrain solutions elsewhere.

As a result, we believe any legislation should be carefully coordinated across the executive branch. We need to move expeditiously to protect the power grid, but let us get this right. The administra-

tion is continuing to examine what additional authorities are appropriate for DOE and the FERC.

To the extent that Congress acts in this area, we recommend that it consider the following: allow the FERC to establish interim reliability standards for the purpose of rapidly responding to specific electric sector vulnerabilities. When presented with a credible cyber threat against the bulk power system, such interim reliability standards could provide an effective bridge until being replaced by cybersecurity reliability standards developed, approved, and implemented pursuant to section 215.

With respect to potential measures in the face of an imminent threat to the bulk power system, allow the Department of Energy to issue an order for immediate remedial action. That order could stand until new FERC interim standards or standards developed pursuant to section 215 were put into place.

Mr. Chairman, that concludes my statement. I am prepared to take any questions.

[The prepared statement of Mr. Kolevar follows:]

STATEMENT OF

KEVIN M. KOLEVAR

ASSISTANT SECRETARY FOR ELECTRICITY DELIVERY AND ENERGY RELIABILITY

U.S. DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON ENERGY AND AIR QUALITY

COMMITTEE ON ENERGY AND COMMERCE

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 11, 2008

Mr. Chairman, members of this committee, thank you for the opportunity to testify before you today on this critically important matter.

This hearing addresses more that just a reliability concern but a national security concern. The Department of Energy and FERC and the electric sector must work cooperatively towards eliminating cyber vulnerabilities in control systems and preventing malicious cyber attacks on our electric infrastructure. Our nation's electric power grid must be better protected – we must harden our power system.

The Department of Energy regularly discovers new vulnerabilities in the control systems employed by many utilities. This is not hyperbole, let me assure you that cyber

attacks against control systems have occurred and they are becoming increasingly sophisticated.

The Director of National Intelligence, J. Michael McConnell, only underscored these concerns when he acknowledged earlier this year that cyber exploitation has not only grown more sophisticated, but more targeted, and more serious. Embedded processors and controllers in critical sectors are being targeted for exploitation and potentially for disruption or destruction with increasing frequency by a growing number of adversaries, not all of whom are in the pay of foreign governments.

According to one senior CIA analyst, some cyber intrusions into utilities have been followed by extortion demands. Cyber attacks have been used to disrupt power equipment in regions outside the United States. And, in at least one case, a cyber-based disruption caused an outage that affected multiple cities.

And because these cyber attacks are conducted over the Internet, they can be launched from just about anywhere, by anyone with a phone line and a modem.

However, while small groups or even individuals could execute limited attacks, a nationwide attack probably would require significant national level resources. Nevertheless, the consequences of a cyber attack on the electric sector are potentially significant, across a host of issues. For that reason, a limited role for the federal government is warranted if the nation's energy infrastructure is to be protected. The nation cannot function without reliable supplies of electricity. Our homes, our communities, our businesses – even the government itself – depend heavily, almost exclusive, on a functioning grid. And we must be increasingly vigilant in our efforts to protect that grid from cyber attacks. To be clear, we must focus on 1) identifying and

eliminating vulnerabilities, 2) improving intelligence gathering and communication of threat information and 3) we must evaluate overall risk and swiftly respond to potential emergencies.

The Department has been substantively engaged on this issue for some time. In 2003, DOE's Office of Energy Assurance, the predecessor program to the current office of Electricity Delivery and Energy Reliability, was designated to work directly with energy owners and operators to protect energy infrastructures from all hazards and help make them become more resilient.

DOE does this by applying sound risk management practices that assess potential weaknesses and we implement physical and cyber solutions to mitigate the risks based on the vulnerabilities we identified.

Under the National Infrastructure Protection Plan's partnership framework, the Department works intimately with the private sector through the Electricity Sector Coordinating Council and the Oil and Natural Gas SCC. In this role, the Department maintains a network of cyber security stakeholders in the private sector and federal, state, local, tribal, and territorial governments.

And this work has spoken directly to cyber concerns. In 2005, the Department collaborated with DHS and Natural Resources Canada to work directly with energy sector asset owners and operators to develop the *Roadmap to Secure Control Systems in the Energy Sector*, a detailed, prioritized plan for cyber security improvements in control systems over the next 10 years.

This effort built trust with the energy sector and has since spawned numerous collaborative efforts to enhance control systems security. More than 100 public and

private projects in the energy sector have been aligned with the Roadmap goals. Control systems cyber security projects funded by the Department of Energy alone have more than 35 private sector partners teaming up with national laboratory researchers.

To date, the Department and its national laboratories have conducted test bed and on-site field assessments of 15 common control systems used widely across the energy sector. These assessments have revealed vulnerabilities ranging in severity from minimal to high impact. Some were one of a kind and were corrected quickly and with relative ease. Others are common to systems found around the country and around the globe, making efforts to address them more complex. In either case, the Department has worked and will continue to work with vendors and asset owners to correct deficiencies, develop security patches and, if needed redesign systems in order to eliminate the identified vulnerability.

The vendors with whom we work are also working to contain the threats. They have developed six next-generation "hardened" systems —one vendor has seen 21 of their hardened systems deployed in the marketplace. And they have released countless software patches to secure legacy systems better.

The Department uses its vulnerability analysis and mitigation to aid the energy sector in implementing sound risk management. Through our national laboratories the Department has conducted cyber security training for more than 1,700 asset owners, operators, and security vendors.

Using knowledge from test bed assessments, the Department educates these end users on cyber security best practices and implementing system fixes and vulnerability mitigation strategies. The Department publishes a periodic "Common Vulnerabilities"

report to educate asset owners and operators on the most common vulnerabilities discovered and actions they can take to mitigate those vulnerabilities on their own systems.

By working directly with vendors and end users for system testing and security training, we have seen an increase in the quality of the partnerships and connections we have developed with the energy sector over the past five years. We understand that securing the energy sector requires maintaining open and close communication with private sector asset owners and operators, who own more than 85 percent of the nation's energy sector assets.

We are vigilant – but our comprehensive understanding of the nature of the threat we face must be updated on a continuing basis. The Department of Energy has long been a source of credible threat information for the nation's energy community. It is part of our job to help them prioritize risk and respond appropriately.

We are constantly leveraging an extensive intelligence-gathering network, proven methodologies, and highly skilled professionals to assess and interpret threat information. With 17 testing facilities from five Department of Energy National Laboratories, we have at our hands field-scale operational and multi-sector control systems for risk assessment, vulnerability testing and advanced modeling and simulation of the impacts and consequences of a cyber attack.

In addition, I am confident we have the necessary intelligence information, analysis capabilities, technical expertise and energy industry relationships to enable us to respond to emerging threats quickly and to make informed decisions that will keep the grid protected, whether problems are the result of cyber attacks or not.

The Administration is continuing to examine what additional authorities are appropriate for DOE and FERC. To the extent that Congress acts in this area, we recommend that it consider the following:

Allow the FERC to establish Interim Reliability Standards for the purpose of rapidly responding to specific electric sector vulnerabilities.

When presented with a credible cyber security threat against the bulk power system, such interim reliability standards could provide an effective bridge until being replaced by cyber security reliability standards developed, approved and implemented pursuant to section 215.

With respect to potential measures in the face of an imminent threat the bulk power system, allow the Department of Energy to issue an order for immediate remedial action. That order could stand until new FERC interim standards, or standards developed pursuant to section 215 were put into place.

The authority to issue emergency cyber security actions is very similar to the Secretary of Energy's existing authority to issue emergency interconnection orders under section 202 of the Federal Power Act. Since 1977, when the Department of Energy Organization Act created both DOE and FERC, the FPA section 202 authority has been vested in DOE. Throughout Administrations involving several different Presidents and of both parties, the Department has used this authority judiciously but effectively to address particular situations in which such an order was necessary to help ensure reliable supplies of electric energy. The Department has demonstrated that, as circumstances warrant, it can exercise the section 202 emergency interconnection authority very quickly.

At this time, Mr. Chairman, I would like to submit my prepared statement for the record and I would be happy to take any questions you may have.

Mr. BOUCHER. Thank you very much, Mr. Kolevar. Mr. Kelliher, I am going to direct my questions to you, and I would appreciate your turning, if you have the information there, to the audit, which the NERC conducted of the 1,200 entities connected to the bulk power system that received the FERC advisory recommending certain steps that should be taken to enhance protection against cybersecurity threats and outlining a schedule of either 90 days in the case of some steps or 180 days in the case of other steps, by which those protections should be put in place.

You audited a number of those 1,200 entities. As I recall, that number was 30. Is that correct?

Mr. KELLIHER. Yes sir.

Mr. BOUCHER. With regard to those 30 audited companies, how many did you find that were at the time of your audit in full compliance with the advisory that had been issued by the NERC?

Mr. KELLIHER. Seven of the 30, sir.

Mr. BOUCHER. So seven of the 30 were in full compliance? Of the remaining 23, had some of those taken some steps toward compliance but were not in full compliance? Or were there any among those 23 that had taken no steps at all?

Mr. KELLIHER. I believe all of the 23 took some steps. It varied on how many they took.

Mr. BOUCHER. How many would you classify, based on your audit, as still being vulnerable to the Aurora vulnerability determined by the Idaho laboratory?

Mr. KELLIHER. Well, that is a more difficult question because full compliance with the advisory itself, in our view, wouldn't necessarily mitigate the Aurora threat. So you are really asking, which companies went beyond the advisory to take steps broader than what NERC had recommended. And that we would say two of the 30 had mitigated the Aurora threat.

Mr. BOUCHER. Leaving 28 still vulnerable in FERC's view?

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER. OK, talk a little bit about what you found in terms of the compliance schedules that had been adopted by the various utilities. Did some of them have truly extraordinary schedules extending over many years as compared to the NERC advisory, which was that these steps be put in place within 180 days?

Mr. KELLIHER. Yes sir, and I think there was some confusion in some of the companies between the timelines in the NERC advisory and the scope of facilities affected covered by the NERC advisory with the rules that the Commission issued, the cyber standards that the Commission approved in January, which envisioned a longer time frame than the NERC advisory. Some companies incorrectly assumed that the longer timelines in the FERC rule govern their compliance with the NERC advisory.

Mr. BOUCHER. So they really didn't understand the NERC advisory?

Mr. KELLIHER. Some of them certainly did not understand the timelines of when their actions were supposed to take place.

Mr. BOUCHER. All right, did you find that there were utilities that had done little or nothing in compliance with the NERC advisory other than simply preparing for the FERC interview that was a part of your audit?

Mr. KELLIHER. They readily participated in our review, so I think the industry gets credit for openly participating. They did ask for some confidentiality, and because they are providing this information voluntarily, we agreed to that. In some cases, I don't think there was a sufficient understanding of what facilities really should be covered by the NERC advisory. I think companies thought they could freely determine if facilities were not part of the bulk power system and were therefore not covered by the advisory, and then shrink the scope of facilities where they might have to act to protect cybersecurity.

In other cases, there was a lack of appreciation for the communication among their facilities. Many and really most electric facilities are capable of remote operation, and some utilities didn't seem to appreciate how interconnected some of their facilities were.

Mr. BOUCHER. And so I gather from that answer that there were utilities that incorrectly assumed that their equipment was not vulnerable to the Aurora vulnerability, when, in fact, you could readily see that that equipment was subject to that vulnerability?

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER. Did you find any entities that excluded critical assets from the implementation to the extent they were implementing the NERC advisory that should have, in fact, been covered and been a part of that implementation?

Mr. KELLIHER. Yes, sir, we think some facilities should have been included that were not.

Mr. BOUCHER. Let me ask for your reasoning, briefly stated, on some of the key issues that we have detected as remaining outstanding where there is some difference of opinion among interested parties with regard to the discussion draft that we have put forward. Specifically the definition of what constitutes a cybersecurity threat, whether or not the authority that is extended to the FERC should go beyond protecting against cybersecurity attacks to protecting against physical attacks to those facilities, whether or not—I am sorry—the conditions under which there should be a sunset on the emergency powers that would be granted upon a Presidential or Secretary of Energy designated emergency?

And then finally, the scope of the authority granted to you in terms of its basic coverage. Should it extend beyond the continental bulk power system to the States of Alaska and Hawaii? Should it extend to major distribution systems in our largest cities such as New York and Washington, D.C.? And I realize that is a question that could occupy a half hour in response. What I am asking for is maybe a 3-minute response if you could.

Mr. KELLIHER. OK, I will do my best. In terms of threshold, I think the threshold in the bill is appropriate. If the threshold is set so high that it is virtually impossible for the President or the Secretary to make a threat determination, then it is probably better not to legislate in the first place because you will end up with a statute that becomes somewhat of a dead letter.

With respect to scope of facilities, we think the scope is appropriate, but it is important for the subcommittee to understand that it is not true that the only cyber threat to the U.S. electricity system is directed at the bulk power system. It can be directed towards other transmission facilities that are not part of the bulk

power system. It can be directed towards local distribution facilities.

In part, we support the current scope because from FERC's point of view, that is what you entrusted to us 3½ years ago. You said FERC, you are responsible to assure reliability of the bulk power system, not the entire electricity system of the United States. We are sticking with what you entrusted to us 3 years ago. We think that scope is appropriate, but we don't want the subcommittee to think that is the only part of the U.S. electricity system that is at risk.

You had four questions. That was only two of them. The——

Mr. BOUCHER. Well, also the conditions under which there could be a sunset on the emergency power.

Mr. KELLIHER. The sunset? I frankly don't think a sunset is appropriate because we are talking about emergency powers and national security law. And FERC isn't usually associated with emergency powers, and I think a sunset is inconsistent with the exercise of emergency power.

Mr. BOUCHER. Well, if the emergency subsides, then obviously the powers associated with addressing that emergency would no longer be necessary.

Mr. KELLIHER. Yes, sir, but I think part of it is how likely do you think the President or the Secretary of Energy would be to declare a threat? If the threat subsided, I think the President and the Secretary would be ready to acknowledge that the threat had subsided. And then the FERC action would terminate.

Mr. BOUCHER. Well, it sounds like your answer to that question is upon a Presidential or Secretary of Energy determination that the threat has ended—because some of the other proposals would have automatic termination——

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER [continuing]. Upon a period of 1 year——

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER [continuing]. As an example unless the emergency was reviewed by affirmative action of the executive. And so your thought on that would be what?

Mr. KELLIHER. I think a sunset is workable, but I think it is inconsistent generally with national security law and the exercise of emergency powers. And you have one more question I haven't gotten to, sir, but I——

Mr. BOUCHER. The definition of what constitutes an emergency——

Mr. KELLIHER. OK.

Mr. BOUCHER [continuing]. And the notion of substantially as a part of the statutory definition.

Mr. KELLIHER. We support the "or" configuration not the "and" configuration because we think the "and" configuration just sets the bar too high.

Mr. BOUCHER. That is too limiting in your view?

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER. All right, thank you. One other question I have.

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER. Did you estimate while you were undertaking your audit of entities attached to the bulk power system what the

cost of complying with the FERC advisory would be for the typical attached entity? That is a key consideration. If it is a minor cost, then there would be little reason for noncompliance to have occurred certainly to the extent that it did.

If it is a major cost, then obviously a different set of considerations begin to apply, and that would necessarily affect timeframes that you would want to have in your order or that we might want to have in the statute for obtaining compliance. So the question of cost is relevant. As a part of your audit, did you address that question? And if so, do you have an estimate of what the cost of compliance per covered facility would be?

Mr. KELLIHER. We do not have a good estimate of what the cost of compliance would be. One aspect of FERC being the actor in this area is that FERC is a regulatory agency, and we can provide for cost recovery. And I think that is an important consideration to industry. And we don't regulate all parts of the electricity industry—I wanted to make sure Sue Kelly heard me say that.

Mr. BOUCHER. It is an important concern to industry, but a larger concern that we take into consideration is the ultimate cost to the energy——

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER [continuing]. User as well.

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER. And cost recovery simply shifts it downward——

Mr. KELLIHER. I agree.

Mr. BOUCHER [continuing]. To the ultimate user, and that is something we would need to consider. So——

Mr. KELLIHER. Yes, sir.

Mr. BOUCHER [continuing]. One thing that I would be very interested in learning, and perhaps other witnesses in their opening statements could address this, is what that estimated cost would be. My time has been grossly exceeded here. Mr. Kelliher, you have been very helpful. I thank you and recognize the gentleman from Michigan for his questions.

Mr. UPTON. Thank you again for your testimony this morning. I do have a couple of questions. And for me again, I am very anxious for our classified briefing with perhaps a few more parties that can help us with this issue so that we can appropriately so come up with the absolute best vehicle.

And of course, as I think back, it was the blackout through much of the Midwest that really prompted the '05 bill. That was the engine that drove the train, bringing about those reliability standards which passed on a pretty broad bipartisan basis. Both Mr. Dingell and Mr. Barton had key roles. They supported the bill. The same thing was in the Senate. I was a part of that conference, and we are glad to see it happen.

And I guess if I had to use an analogy, I raised about the FAA towers, the FAA control back on 9/11 today ordering all the planes to come down. In essence, you all can send out advisories, but you can't enforce what you have to say. So it would be very much along what American Airlines was told a few months ago when they literally had to shut down their airline as they had to rebundle all of those wiring packages in their planes because the advisory came out. And those planes couldn't fly until it was done. And in essence,

I would think that we need to make sure that you have the power to, as you issue those advisories, to make sure that they are completed in a timely manner.

And in response to Mr. Boucher's question about cost, I suppose as part of that advisory, you could ask the utilities what they anticipate those costs to be. Is that not something that you do now then in terms of the advisories that go out or not?

Mr. KELLIHER. Certainly with respect to any action we take to mitigate the Aurora threat, that would be through a notice and comment rulemaking, and the industry would certainly raise cost in the context of that rulemaking.

Mr. UPTON. What type of trigger would you mean? As we think about Jim Langevin, our colleague who spoke earlier in terms of the chain of command. And one of the issues that he raised was that it may happen so fast, cyber seconds, you may not have time to go to the whatever chain of command that you have, whether it be the NSA, the President, the Secretary of Energy. What type of pre-trigger would you suggest be employed for you to I would suppose, what shut down a utility or shut down part of the grid to make sure that it doesn't expand? Is that the type of threat that you would envision would happen?

Mr. KELLIHER. Let me try to come up with a hypothetical that could try to put it in place, and hypotheticals are sometimes useful, sometimes not helpful. But I will take the risk. Let us assume that the Department of Energy or the President or somewhere in the National Security Agency, they identified some threat to substations in a city. There was some effort to destroy substations, and the President or the Secretary made a finding consistent with the statute, that there is a credible—I don't actually remember the exact words—but the President or the Secretary made a finding consistent with the statute.

FERC would not be in a position to make that finding because we are not an intelligence agency. But upon that finding, we could theoretically identify where there are spare transformers in a country. We could theoretically order them to be relocated to that metropolitan area in anticipation of a possible attack. And we could also allow for cost recovery for the owners of those transformers, if they are regulated entities. And we could try to come up with a creative approach to address cost recovery if they are not.

That is the kind of thing that conceivably we could do under this scenario. In an urban area, we could order generators to have higher spinning—to operate their system differently to basically have more generation on call in the event some facilities were damaged or destroyed.

So there are operational changes that we could order. We could order the relocation of spare transformers, and there would be other hypotheticals as well.

Mr. UPTON. That would take time though. I mean that would actually be something—by the time you located a generator and move it to the right spot, it could——

Mr. KELLIHER. Not the second one. Ordering generators to have higher spinning reserve levels, that is something that could be done immediately.

Mr. UPTON. You know, as I think about what happened back in '05—and remember I am from Michigan——

Mr. KELLIHER. Yes, sir.

Mr. UPTON [continuing]. So go like this. And I live over here, and we have two nuclear plants, and I can remember one of our plants, the Palisades plants, they were within less than a minute of shutting that facility down because of the drain on the network from Columbus and Ohio and other places. It was just sucking the power through the grid, and had that shut that plant down, it would have gone right around the horn over to Chicago. And it would have been even far worse. So they had to make the decision as to whether they were going to keep it online. And thank goodness they didn't have to hit the shutoff button, which who knows how long. It would have been much longer, much more in damages in terms of what would have happened.

But that was their own independent decision as to whether they were going to—and I think it was Consumers Energy then owned it. It could have been Entergy, but it was that nuclear plant that, because it stayed on, actually prevented it from going and hitting even more of the Midwest than what happened.

But as I recall that was their own independent decision. It wasn't FERC that told them to shut it down or somebody else. And I don't know if the '05 act would change that, who would enforce it. If it was a cyber act, you would think that again it would be pretty—whoever the president would be would take almost immediate action to try and prevent damages or loss from expanding beyond perhaps individual facilities which would trigger even broader blackout for who knows how long.

Mr. KELLIHER. That kind of scenario in terms of the 2003 blackout, that might—I am not familiar with the particular circumstances of that nuclear plant. But that is something that could be covered by the reliability standards that the Commission approved a year-and-a-half ago. But if——

Mr. UPTON. But who would give that order? I mean would you—are you able now to enforce——

Mr. KELLIHER. I think——

Mr. UPTON [continuing]. Have some enforcement action?

Mr. KELLIHER. I can't say with certainty that there is a current reliability standard that would govern the decision by a nuclear plant whether or not to continue to operate because nuclear plants—there are standards that the NERC establishes, the governing loss of offsite power. And nuclear plants, I think they generally do shut down when they lose offsite power.

So we have tried to synch up our reliability standards with NERC standards, and we wouldn't want to interfere with NERC safety standards.

Mr. UPTON. Yes, I wonder if we should have the NERC as a participant in our meeting next week. Probably should. So I have gone beyond my time as well, so I yield.

Mr. KOLEVAR. Mr. Chairman, if I can respond to the Congressman's question as well. When we look at this, there are really probably three situations that we need to think about when we are talking about threats to the grid and then immediate reliability implications and long-term reliability implications.

Congressman, I think the situation you described falls into the latter category. Those are actions that the utilities would take or that the operators at that nuclear facility would take as a result of the standards development process.

When we are looking at the draft legislation today at the Department of Energy, we really seek two other scenarios. One is you have a credible threat probably against a specific facility or a portion of the grid that requires immediate action. The Department of Energy does exercise some similar emergency authorities for the purposes of interconnection in particular. And that can be issued in about an hour. I think the FERC actually has some similar authorities to 202C that are able to be executed very quickly.

So that is your imminent immediate threat to which the Federal Government must take action and respond and give direction to the sector.

The second is the situation that I think Aurora exemplifies, and that is a vulnerability. But the risk of exploitation of that vulnerability is relatively low. You don't have a player. You don't have a time. You don't have a specific threat. And in that type of situation, that does speak to an interim authority at the FERC over a period of 90 days, 120 days, 6 months, whatever it is that the commission of the utilities decide is most appropriate to speak to that threat and identify the interim standards that are going to be employed to ensure that that threat can't be exploited.

Mr. UPTON. Thank you.

Mr. BOUCHER. Thank you very much, Mr. Upton. The gentleman from Oregon, Mr. Walden, is recognized for 5 minutes.

Mr. WALDEN. Thank you very much, Mr. Chairman. I think it is appropriate we are having this hearing today because I think for some of us this issue really came to life in a post-9/11 environment, some of the briefings that we had at that time. And for those of us in the West with the long interconnection ties, I think of my district in Oregon where we ship the power from the hydro system through those big DC converter lines down to California at all. That there are enormous vulnerabilities and opportunities for mischief, if not downright destruction.

And I guess, Mr. Kelliher, I would like to ask a couple of questions. One involves this—and I have had no classified briefings on this. So if I stumble into an area I don't belong, shut me down. That is fine. But it would seem to me that, if there is a cyber threat, is the issue that they can do a phase shift then and modify the power itself and cause disruption in the transformers. Is that part of it? Can they do voltage spikes? Blow up the transformers? What sorts of issues do we need to be aware of here?

Mr. KELLIHER. It is probably better to say they can cause physical damage and actually destroy facilities like transformers, and there are different ways they can—a cyber attack could cause that damage.

Mr. WALDEN. And then when it comes to the destruction of transformers, because that could be done with a explosive device. I mean today somebody could go out out to one of those substations and do damage. Have we in the interceding 7 years taken stock of sort of our transformer supply? Because my understanding is that it could take months if not perhaps longer than that to replace some

of these transformers if you had to start over from scratch and build them. Is that correct?

Mr. KELLIHER. We have taken the first steps at FERC to encourage the development of spare transformers.

Mr. WALDEN. OK.

Mr. KELLIHER. Because, as you say, transformers, they can take months, perhaps a year or longer actually to manufacture. And there generally are not very many spare transformers in the United States.

Mr. WALDEN. They are very expensive.

Mr. KELLIHER. They are very expensive. So we have issued an order that would provide for cost recovery to the extent regulated companies develop spare transformers so that they could then be pooled for use.

Mr. WALDEN. And do you know are there companies taking advantage of that?

Mr. KELLIHER. I don't know the status of whether there has been an increase in the purchase of transformers. We have an order that allows for cost recovery. I don't know what has followed the issuance of our order.

Mr. WALDEN. Because I can see an oversight hearing post some event where we question the utilities about why they didn't take advantage of that and have at least some sort of backup. I realize you are not going to have one for one. I fully understand that, but it would seem to me that is an area where we would need backup because isn't the alternative that the grid could be down for a long period of time?

Mr. KELLIHER. Certain facilities can be damaged or destroyed, and that is different than a blackout scenario where you can recover relatively quickly. Recovery could take longer in the wake of a successful cyber attack.

Mr. WALDEN. Or a physical attack.

Mr. KELLIHER. Yes, sir.

Mr. WALDEN. Either one. So it would seem to me that, one, we need to investigate more in terms of where utilities are in backup transformers because that just seems logical to me. Just as you have generators ready to go in case there is a hurricane somewhere or any other disaster. This notion of having backup transformers would certainly make sense.

This other issue about having to have a presidential declaration and all. It would strike me—and perhaps, Mr. Kolevar, you can address this as well—that if a utility or grid manager got word that there is some potential cyber attack, wouldn't they want to react instantly to stop any damage to their systems?

Mr. KOLEVAR. I would expect they would.

Mr. WALDEN. And I heard some reference that it could take upwards of an hour perhaps. Why would it take that long?

Mr. KOLEVAR. Your question goes to the actions that the utility——

Mr. WALDEN. Right.

Mr. KOLEVAR [continuing]. Upon information——

Mr. WALDEN. Like shutting down a nuclear plant.

Mr. KOLEVAR [continuing]. Would take. My experience with the electric sector is they would take immediate actions to protect their

system. They do that now when they have anomalies on the grid. To the extent that you are talking about an emergency order issued by the Federal Government—and for our purposes, we think the analogous order is a section 202C order under the Federal Power Act where the Secretary of Energy finds that an emergency exists in the sector, and that might be because of a natural disaster. The hurricanes that hit in 2005——

Mr. WALDEN. Right.

Mr. KOLEVAR [continuing]. Caused one. Or we have a reliability emergency, which was the case in the order that was issued for the local Mirin plant on the Potomac River. And the point is to say that where there is a need to act quickly with Federal orders speaking to the operation of a system, that there is a history of the Federal Government moving very quickly from administration to administration in preparing and releasing an order to the electric sector to respond accordingly.

Mr. WALDEN. All right, Mr. Chairman, I know my time has expired, and I know we have been joined by my colleague from Illinois. So I would thank you for your indulgence.

Mr. BOUCHER. Thank you very much, Mr. Walden. The gentleman from Illinois is welcomed to the subcommittee today, and Mr. Shimkus is recognized for 5 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. I was on the floor, as you know, fighting for coal. Thought you would appreciate that.

Mr. BOUCHER. Did you bring some with you?

Mr. SHIMKUS. Right here. It is good southern Illinois coal.

Mr. BOUCHER. We talked about coal a lot in this subcommittee. I am not aware we have actually had it here before.

Mr. SHIMKUS. Well ——

Mr. BOUCHER. I thank the gentleman.

Mr. SHIMKUS. We need a new good electric grid for all that Illinois coal to be used in electricity generation and spread to lower prices for all over the country, Chairman. I am unprepared to follow up with concise questions. So I will just yield back, Mr. Chairman.

Mr. BOUCHER. Well, you will have your opportunity on the second panel, and I thank the gentleman. Mr. Kelliher, did you care to make another remark?

Mr. KELLIHER. Mr. Chairman, I just wanted to clarify my earlier comments about the sunset. I do think generally a sunset is inconsistent with the use of emergency powers, but FERC has, in our discussions with industry groups and with others, agreed to a sunset in the scenario where if there would be a Presidential finding or a finding by the Secretary, FERC would be directed to act. We have agreed to a 1-year sunset in the course of discussions in order to develop the broadest possible consensus. So I just wanted to clarify my comments on sunset.

Mr. BOUCHER. And then on the question, Mr. Kelliher, of the basic powers that the statute would confer upon FERC, that would not be subject to a sunset? The basic requirements that the facilities connected to the grid take certain steps, all of them take certain steps as a basic protection against cybersecurity would not be subject to sunset. It would only be the emergency powers that are granted pursuant to special Federal finding, Presidential finding

that there is a unique emergency that would be subject to some sunset?

Mr. KELLIHER. Yes sir, and the permanent standards that we have established under section 215 would not sunset, would not be affected. It would be the emergency actions, if you will.

Mr. BOUCHER. Thank you for that clarification. It is very helpful. Mr. Kolevar, Mr. Kelliher, I know that both of you have urgent obligations elsewhere. We thank you for your attendance this morning, and you are excused.

We now turn to our remaining witnesses on the panel who have already been introduced. And we would ask that your oral statements be kept to approximately 5 minutes, and that will leave us ample time for questions. Mr. Sergel, we will be happy to begin with you.

STATEMENT OF RICHARD P. SERGEL, PRESIDENT, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. SERGEL. Thank you, Mr. Chairman and members of the subcommittee. My name is Rick Sergel, and I am the president of the North American Electrical Reliability Corporation, known here as NERC. I appreciate the opportunity to appear before you today on this very special day and on this very important topic.

Let me be clear: the risk to the operation of the Nation's electricity system from potential intrusion through the Internet into computerized system control capabilities, AKA cybersecurity attacks, is real. It is not new. The Energy Policy Act of 2005 in which this committee played a major role and which, for the first time, authorized the promulgation and enforcement of mandatory reliability standards to protect the bulk power system defined reliability standards as specifically including cybersecurity protection. You identified that early on.

But at the same time, the nature of the threat is new every day because it changes all the time. And as the entity entrusted with protecting the reliability of the North American bulk power system, subject to FERC oversight in the United States, NERC takes very seriously its responsibilities for protecting the cybersecurity of the North American bulk power system and meeting this ever-evolving threat.

NERC now has the ability to enforce over 100 reliability standards, including nine dealing with cybersecurity. These standards have improved the reliability of the system, including its cybersecurity.

However, cybersecurity threats are different from other reliability concerns. Potential threats can arise very quickly, requiring rapid, effective, and often confidential responses. Cybersecurity threats are more likely to be driven by intentional manipulation of devices as opposed to operational events in the bulk power system, such as lightning or equipment malfunctions.

When there is an imminent cybersecurity threat, the response must be immediate. It must provide for confidential treatment of critical information, rapid threat analysis, and directed actions necessary to address the threat.

NERC develops reliability standards using a transparent process that provides for full participation of interested parties and draws

heavily on industry expertise, but this takes time, and it takes transparent exchanges of data and views that are not well suited for a cybersecurity threat.

For these reasons, it is NERC's position that in the event of an imminent cybersecurity threat, the U.S. Government should be authorized to act immediately. With emergency responsibilities in the hand of government, NERC will be better able to do what it does best. That is develop and implement cybersecurity reliability standards that will harden the grid against intrusion and aid in responding effectively to cybersecurity incidents.

NERC is committed to ensuring the reliability of the system and assuring that NERC's efforts will be complementary to those of government and industry with regard to cybersecurity protection. Finally, NERC is committed to assuring that there are no gaps and that responsibility is clear for execution of cybersecurity protection initiatives.

With helpful guidance from Chairman Langevin, NERC has elevated the importance and the urgency of understanding and addressing cybersecurity threats. Key elements of this strategy include consolidating responsibility for coordination of all cybersecurity matters across all NERC activities into a single responsibility area lead by our new chief security officer, Michael Assante, who is here with me today.

Improving our standards and developing processes to enable us to set standards on a more expedited basis are also important, as well as: raising the importance of the issue within the industry by engaging CEOs at the strategic and policy setting level; communicating more effectively with industry on critical infrastructure security matters; and coordinating effectively with the multiple government stakeholders involved in protecting the grid from cybersecurity attacks. You have talked about that several times this morning.

In summary, cybersecurity threats to the bulk power system are real. Working with the government and industry, NERC is committed to addressing these threats; however, in order to address an imminent cybersecurity threat, the Federal Government must have emergency authority to act.

NERC commends the subcommittee's efforts to develop appropriate emergency legislation and pledges to assist in this effort in any way that we can.

Several times this morning, you have discussed our actions with respect to responding to Aurora, I think it is fair to say that when we acted with respect to Aurora by issuing our advisory, we did do some good. There has been progress as a result of sending that out, and we did the right thing to send it out. We also demonstrated, and for NERC painfully, the limitations of that process. There are limitations with respect to every aspect of it, including who did it go to. You mentioned numbers here today, 1,200, 1,500. I am uncomfortable with all of those because we know so much better who the individuals are that should get that advisory today than we did at that time.

But the most important thing that we demonstrated was the limitation of trying to use a voluntary standards process and thinking that it could deal with an emergency threat. We recognize that

there is a better way to do that and would ask you to establish legislation that can make that happen. Thank you very much.

[The prepared statement of Mr. Sergel follows:]

Summary of the Testimony of Richard P. Sergel, NERC
Before the Energy and Air Quality Subcommittee
September 11, 2008

The North American Electric Reliability Corporation (NERC) takes most seriously its responsibilities for protecting the cyber security of the North American bulk power system. Working with our stakeholders, our job is to protect the reliability of the grid, and cyber security is an important element of that responsibility. But the challenges the grid faces from cyber security threats are different from other reliability concerns. Cyber technologies change frequently and potential threats can arise very quickly, requiring rapid, effective and often confidential responses. Threats can arise anywhere across the vast array of communicating devices on the grid -- Supervisory Control and Data Acquisition (SCADA), control rooms, power plants, substations, relays, meters, some transformers, capacitor bank controllers, to name just a few – and the systems to which those devices are connected. Cyber security threats are more likely to be driven by intentional manipulation of devices as opposed to operational events on the bulk power system.

All of these challenges set cyber security apart from other reliability concerns. When there is an identified, immediate threat, the response must also be immediate. It must provide for confidential treatment of critical information, rapid threat analysis, and directed actions necessary to address the threat. For these reasons, it is NERC's position that in the event of an imminent cyber security threat, the U.S. government needs authority to act immediately. With emergency responsibility in the hands of government, NERC will be better able to do what it does best: develop and implement cyber security Reliability Standards that will harden the grid against intrusion and aid in responding effectively to cyber security incidents.

NERC in collaboration with the industry is committed to 1) ensuring the reliability of the bulk power system in the face of cyber security threats; 2) assuring that NERC's efforts will complement those of the government and industry with regard to cyber security protection; and 3) assuring that there are no gaps and that responsibility is clear for execution of cyber security protection initiatives.

NERC has elevated the importance and the urgency of understanding and addressing cyber security threats. Key elements of this strategy are:

- consolidating responsibility for coordination of cyber and all other security matters across all NERC activities into a single responsibility area led by a new Chief Security Officer;
- developing an emergency/crisis standards setting process;
- expanding the strategic and policy guidance provided by and to industry executives on critical infrastructure security matters; and
- working to coordinate more effectively with the multiple government stakeholders.

Cyber security threats to the bulk power system are real. Working with the government and industry, NERC is committed to addressing these threats.

TESTIMONY OF RICHARD P. SERGEL
PRESIDENT AND CHIEF EXECUTIVE OFFICER
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BEFORE THE SUBCOMMITTEE ON ENERGY AND AIR QUALITY
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

Hearing on
PROTECTING THE ELECTRIC GRID FROM CYBERSECURITY THREATS
September 11, 2008

INTRODUCTION

The North American Electric Reliability Corporation (NERC) takes most seriously its responsibilities for protecting the cyber security of the North American bulk power system. Working with our stakeholders, our job is to protect the reliability of the grid, and cyber security is an important element of that responsibility. But the challenges the grid faces from cyber security threats are different from other reliability concerns. Cyber technologies change frequently and potential threats can arise very quickly, requiring rapid, effective and often confidential responses. Threats can arise virtually anytime and anywhere across the vast array of communicating devices on the grid – Supervisory Control and Data Acquisition (SCADA), control rooms, power plants, substations, relays, meters, some transformers, capacitor bank controllers, to name just a few – and the systems to which those devices are connected. Cyber security threats are more likely to be driven by intentional manipulation of devices as opposed to operational events on the bulk power system.

All of these challenges clearly set cyber security apart from other reliability concerns. When there is an identified, immediate threat, a different approach is required

– one that allows for more expedient and confidential treatment of critical information, rapid threat analysis, and directed action on necessary actions. For these reasons, we believe that in the event of an imminent cyber security threat, the U.S. government needs immediate authority to act. With the immediate emergency responsibility in the hands of government, NERC will be better positioned to do its job of developing and implementing cyber security and critical infrastructure protection Reliability Standards that will harden the grid against intrusion and aid in responding effectively to cyber security incidents.

My testimony today will focus on the steps that NERC is taking to enhance protection of the grid from cyber security threats.

I. BACKGROUND

NERC's mission is to ensure that the bulk power system in North America is reliable. To achieve this objective, NERC develops and enforces Reliability Standards that are now mandatory, thanks to the Energy Policy Act of 2005; monitors the bulk power system; assesses and reports on the adequacy of electricity supplies and transmission; and educates, trains and certifies industry personnel. NERC, which draws upon the collective expertise of the electricity industry, is subject to oversight by the Federal Energy Regulatory Commission (FERC) in the United States and by governmental authorities in Canada. FERC certified NERC as the Electric Reliability Organization (ERO) in July 2006.[1] Most Reliability Standards approved by NERC and FERC became mandatory and enforceable in June 2007.

[1] *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

On January 18, 2008, FERC issued Order No. 706, approving eight mandatory Reliability Standards for Critical Infrastructure Protection (CIP Reliability Standards).[2] Approval of the CIP Reliability Standards was a major step forward in ensuring the reliability of the electric grid because these standards set forth specific requirements that are binding on users, owners and operators of the bulk power system to safeguard critical cyber assets. They require identification and documentation of cyber risks and vulnerabilities, establishment of controls to secure critical cyber assets from physical and cyber sabotage, reporting of security incidents, and establishment of plans for recovery in the event of an emergency.

The Critical Infrastructure Protection Reliability Standards approved through Order No. 706 are a sound starting point for the electric industry to address cyber security. Improvement of the CIP Reliability Standards, however, already is underway, both in response to directions given by FERC in Order No. 706 and as part of NERC's ongoing Reliability Standards development process.

II. NEW FEDERAL AUTHORITY TO DEAL WITH CYBER SECURITY EMERGENCIES IS NEEDED

The NERC standards development process is designed to respond to defined, measurable risks that can be identified from operating experience, event analysis, compliance audits, system and equipment performance analysis, and benchmarking programs. The process is structured to leverage industry subject matter expertise against well defined problems with long histories and defined data. This process responds to a need for standards that is transparent, relatively well known and widely understood.

[2] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 122 FERC ¶ 61,040, *reh'g denied,* Order No. 706-A, 123 FERC ¶ 61,174 (2008).

Incremental improvement in standards over time is acceptable for many Reliability Standards.

In contrast, addressing cyber security attacks may require significant change without operating experience as a basis and in very short timeframes. Just as SCADA and communications technologies change frequently, potential threats also arise quickly. Standards relating to critical infrastructure in general, and cyber security in particular, must continue to evolve, but that evolutionary process may not be adequate to respond to an immediate threat. Moreover, the open process by which Reliability Standards are developed, while demonstrably successful in producing standards that have significantly enhanced the reliability of the grid, may not be ideally suited to situations where, because of the sensitive subject matter, confidentiality is required and time does not permit extensive consultation.

The intentional nature of cyber and physical security threats means the protection of the bulk power system is dependent in large measure on the quality and timeliness of threat analysis and risk assessments developed by others outside the electric industry. Classified intelligence information, rather than the observable operating conditions of the bulk power system, can quickly raise the threat level.

NERC draws much of its technical expertise from the collective wisdom of industry volunteers, assembling industry subject matter experts into drafting teams, developing and posting proposed standards for broad industry stakeholder comment, and gaining approval by supermajority vote. For the majority of Reliability Standards, this inclusive process works to elicit the data and information needed for Standards development; however, with respect to cyber security threats, much of the critical

information resides within government agencies and confidential treatment of that information is essential. In non-emergency situations, NERC can coordinate with the appropriate agencies and the limitations associated with confidential information can be managed. Existing authorities and established processes enable both a comprehensive risk assessment and the development of strategies and plans to address those risks to the security of the bulk power system. However, in the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government.

III. NERC'S ROLE IN PROTECTING AGAINST CYBER SECURITY THREATS

NERC reviews cyber security threats on an ongoing basis. NERC's Critical Infrastructure Protection Committee (CIPC),[3] has coordinated NERC's security initiatives for several years. The CIPC Executive Committee, along with the NERC CEO and Chief Security Officer, serve as the Electricity Sector Coordinating Council to collaborate with the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) on critical infrastructure and security matters. Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[4] which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

[3] CIPC is comprised of industry experts in the areas of cyber security, physical security, and operational security. CIPC reports to NERC's Board of Trustees. It is governed by an Executive Committee, whose members manage CIPC policy matters and provide support to CIPC's subcommittees and their working groups and task forces.

[4] The ES-ISAC has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC works with the electricity industry to identify and mitigate cyber vulnerabilities by providing information, recommending mitigation measures, and following up to monitor implementation of recommended measures. NERC, in its capacity as the ES-ISAC, also has some related responsibilities for cyber and physical security issues associated with all electric facilities operated in the United States.

NERC and the industry share a mutual goal to ensure that threats to the reliability of the bulk power system, especially cyber security threats, are clearly understood and are mitigated. NERC in collaboration with the industry is committed to 1) ensuring the reliability of the bulk power system from a cyber security threat; 2) assuring that NERC's efforts will complement those of the government and industry with regard to cyber security protection; and 3) assuring that there are no gaps and that responsibility is clear for execution of cyber security protection initiatives.

NERC has committed to elevating the importance and sense of urgency associated with cyber security threats. Key elements of this strategy are:

Establishment of a Chief Security Officer (CSO) and Creation of a Core NERC Critical Infrastructure Protection Program

Recognizing the critical differences associated with cyber security threats to bulk power system reliability, NERC has consolidated responsibility for coordination of cyber and all other security matters across all NERC activities into a single responsibility area. On September 2, Michael J. Assante joined NERC as "Chief Security Officer." Mr. Assante comes to NERC from the Department of Energy's Idaho National Labs (INL) as a widely recognized expert and visionary in the fields of security and infrastructure protection. He also serves as a member of the Commission on Cyber Security for the 44th Presidency of the United States. Prior to assuming his strategic leadership position at INL, Mr. Assante was a vice president and Chief Security Officer at American Electric Power, one of the largest generators of electric power in the U.S. Mr. Assante thus has the background to lead NERC's cyber security protection program to a new level, and to be a critical point of contact with industry and government. He reports directly to me.

The CSO is responsible for assuring that the Rules of Procedure for all NERC programs are implemented in a timely and effective manner with respect to Critical Infrastructure Protection. He is also responsible for evaluating and recommending any changes to the NERC Rules of Procedure necessary to achieve the objectives of NERC's Critical Infrastructure Protection program. In addition, the CSO is responsible for assuring coordination between NERC and government agencies with respect to all critical infrastructure protection matters, especially where confidentiality is an issue.

As a first step, the CSO, with the assistance of the Regional Entities, will perform an assessment, with metrics and recommendations, of the preparedness of the users, owners, and operators on the NERC compliance registry to address cyber security threats. The assessment and recommendations will address preventing intrusions as well as assessing the capability for isolating and limiting attacks so they remain within our abilities to withstand any subsequent equipment losses and restore the system quickly. The CSO also will represent NERC in the Partnership for Critical Infrastructure Security.

Alternative Standard Setting Process for Cyber Security Standards

NERC has established a task force to review, and where appropriate recommend, a revised standard setting process for cyber security that will include an emergency/crisis standards setting process. This process must provide a level of due process and technical review, but also provide the speed necessary to establish Standards quickly and work seamlessly with any new authority granted in the United States to the FERC. As part of this effort, NERC will investigate and review standards development models from other industries.

Continual Upgrading of Existing CIP Standards

NERC also is working to accelerate the review of the existing CIP Reliability Standards. The Commission in Order No. 706 directed NERC to develop modifications to the CIP Reliability Standards to address specific matters through the Reliability Standards development process. Among other things, NERC is specifically considering the extent to which elements of the Recommended Security Controls for Federal Information Systems under development by the National Institute of Standards and Technology (NIST) can be incorporated into the CIP Reliability Standards. NERC also is developing guidance documents to help entities know what is expected to comply with certain aspects of the CIP Reliability Standards.

Expand Role of Industry Executives at NERC

NERC has formed the Electric Sector Steering Group (ESSG) to provide strategic and policy guidance to the Electricity Sector Coordinating Council and to NERC in its role as the operator of the ES-ISAC. The ESSG includes five CEO-level industry executives, a NERC board member, and the NERC CEO. The five industry executives were selected by NERC's Member Representatives Committee to provide broad stakeholder and geographic representation. Chaired by the NERC CEO, this group will provide high-level policy guidance and broad electricity sector participation and support on critical infrastructure security matters, including matters beyond the bulk power system. This group will be instrumental in providing direction and support for these and future key NERC and industry security initiatives. The ESSG will also provide advice to the CSO as he develops critical infrastructure protection into a core NERC program.

Inclusion of the industry executives will facilitate the peer-to-peer contacts that will be essential to effective implementation of these efforts.

Closer Coordination with Government Stakeholders

NERC, with the guidance of the ESSG, is establishing an enhanced process to conduct comprehensive and continuous assessments of security risks to the bulk power system of North America. Existing risk assessment efforts tend to be focused on individual organizations, but do not provide a complete understanding of the concerns facing the interconnected bulk power system and do not guide industry-wide efforts to develop prudent approaches to address the most material risks. NERC's roles in providing this assessment are to identify areas of concern and to make recommendations to address those concerns in a prioritized manner. This process will follow the sector framework established in the National Infrastructure Protection Plan and will be conducted with stakeholders and appropriate government agencies, including, but not limited to, DHS, DOE, FERC, and their Canadian counterparts. The assessment will serve as a foundation to guide protection goals and strategies to include the future development of Reliability Standards. The assessment will provide a complete landscape of security risks, identify significant trends and provide a common language allowing industry and government to effectively highlight both existing and emerging concerns.

IV. CONCLUSION

NERC is committed to ensuring the reliability of the bulk power system, including with respect to cyber security. NERC's actions are designed to complement those of the government, as well as actions taken by users, owners, and operators of the bulk power system. Through a better understanding of the challenges associated with

cyber security, and a commitment to a world class cyber security program, NERC seeks to enable industry to address the significant challenges to bulk power system reliability posed by cyber security threats.

Mr. BOUCHER. Thank you very much, Mr. Sergel. Ms. Kelly.

STATEMENT OF SUSAN N. KELLY, VICE PRESIDENT, POLICY ANALYSIS, AND GENERAL COUNSEL, AMERICAN PUBLIC POWER ASSOCIATION

Ms. KELLY. Thank you. I am Susan Kelly. I am the Vice President of Policy Analysis and the General Counsel of APPA. And I have with me Alan Mosher, who is our Senior Director of reliability. We represent the interests of more than 2,000 publicly-owned electric systems in 49 States, and we serve 45 million Americans.

Those of you who know our industry know it is rare for our trade associations to speak with one voice on a federal energy policy issue, for legitimate reasons. We generally have very different views. But on the issue of protecting the bulk power system from cybersecurity emergencies, we have come together. APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electric Consumers Resource Counsel, the Electric Power Supply Association, the Large Public Power Counsel, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association, and the Transmission Access Policy Study Group all support carefully crafted specific legislation as the basis to deal with the discrete issue of cyber system emergencies.

We understand the seriousness of the issue and the need to deal with it, but at the same time, we think that legislation needs to be carefully crafted and narrowly drawn.

The subcommittee has asked me to address several issues regarding the House discussion draft. The full answers are in my written testimony, and I will just hit the highlights here. The associations support the House discussion draft with the specific language options that the associations have proposed. As so modified, we think it provides the commission with sufficient authority to deal with cyber system security emergencies.

The draft would fill a narrow gap in the mandatory reliability standards regime that has been set up under section 215. Under that section, FERC has certified NERC as the ERO. With the help of hundreds of industry volunteers, NERC develops and enforces mandatory reliability standards for the bulk power system to keep our lights on. FERC oversees NERC's activities in the United States.

But NERC's standards also apply to utilities in Canada and northern Mexico. This industry-based framework is working to assure the reliable planning and operation of the bulk power system.

Cybersecurity emergencies present a special case for three different reasons. First, they require protection against deliberate, malicious attacks intended to disrupt bulk power system operations. Second, new and unforeseen threats can arise very quickly, leaving little time to react. Third, there is a need for confidentiality, at least until the initial measures are in place. For these reasons, the association supports specific legislation to deal with such emergencies, but it must not undermine the section 215 framework. That framework needs to be able to continue to develop and mature.

The House discussion draft dovetails with section 215. It is limited to the users, owners, and operators of the bulk power system. As NERC has applied that term in practice with FERC's approval, retail customers, local distribution facilities, small generators, and small utilities are generally excluded from the scheme. Any new cybersecurity legislation should apply to the same universe of facilities and entities. To do otherwise would raise jurisdictional and implementation issues that could greatly complicate consideration of this legislation.

State regulatory commissions regulate local distribution facilities. The state's authority to regulate the reliability of local distribution networks and service should be preserved.

I was specifically asked to discuss the remaining differences between the associations and FERC on the House discussion draft. The associations negotiated at length with FERC staff regarding this draft. We reached closure on many issues. We thank the FERC staff for the constructive and positive attitude it displayed throughout the negotiations. We were unable to reach closure on three issues, but that should not undermine the very substantial progress that we did make.

The three areas are, first, the definition of a cybersecurity threat, as you have already heard. The associations and FERC agreed on most elements of that definition, but we think our proposed language limits the legislation to true cybersecurity emergencies, meaning threats that have a substantial likelihood of happening and that could substantially disrupt operations if they do happen. FERC's proposed definition is broader.

The second issue is the inclusion of national security threats. FERC wants to expand the legislation to include "other national security threats" as well as cybersecurity threats. Our associations believe that other government entities, both State and Federal, have more direct responsibility in the general area of national security.

Moreover, this additional authority is quite vague in its wording and potentially all-encompassing in nature. We think including this language would spark an intense discussion that could slow the legislation down.

Third, the sunset of interim measures that FERC enacts. We negotiated at length with FERC on the sunset provisions, and we reached closure on all issues except one. And that has to do with whether the sunset after 1 year unless there is an indication from DOE or the President that it should continue, should apply to both the interim measures under subsection B and the emergency measures under subsection C. Subsection B deals with Aurora. Subsection C deals with what happens thereafter on a going forward basis. We think those measures and orders should be either time limited by their natures or replaced by NERC reliability standards because in the long run, we think the standards should deal with this. FERC doesn't agree with this position.

We couldn't reach closure, but we do think that we made a lot of progress on legislation. As this process moves forward, we strongly urge Congress to retain the carefully crafted language that the associations support. We thank you very much, and we stand ready to answer questions.

[The prepared statement of Ms. Kelly follows:]

Summary of the Statement of the
AMERICAN PUBLIC POWER ASSOCIATION (APPA) for the
HOUSE ENERGY AND AIR QUALITY SUBCOMMITTEE'S
Hearing regarding "Protecting the Electric Grid from Cyber-security Threats"
September 11, 2008

Testimony of Susan N. Kelly

I am Susan Kelly, Vice President of Policy Analysis and General Counsel of APPA. APPA represents the interests of more than 2,000 publicly-owned electric utility systems in 49 states, serving approximately 45 million Americans.

APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association, and the Transmission Access Policy Study Group (associations) all support carefully crafted and specific legislation as the basis to deal with the discrete issue of cybersecurity emergencies. We understand the seriousness of the issue, and the need to deal with it. Any such legislation, however, must be carefully drawn and narrow in its application, to avoid disrupting the mandatory reliability regime that Congress has already required and the electric utility industry has implemented under section 215 of the Federal Power Act (FPA), with the oversight of the Federal Energy Regulatory Commission.

Among other things, such legislation should:

- Be limited in its application to the bulk-power system, as that term is defined in FPA section 215(a)(1);

- Define the term "cybersecurity threats" to limit the reach of the legislation appropriately to cybersecurity emergencies – meaning threats that have a substantial likelihood of happening and that could substantially disrupt the reliable operation of the bulk-power system if they do happen; and

- Be limited to "cybersecurity threats," rather than expanded to include both cybersecurity threats and "other national security threats." The associations believe that other government entities, both state and federal, have more direct responsibilities in the general area of national security. Moreover, this additional authority is quite vague in its wording and hence potentially all-encompassing in nature, which in and of itself raises substantial concerns.

We strongly urge Congress to retain the carefully crafted legislative language that the associations support as the process moves forward.

American Public Power Association

1875 Connecticut Avenue, NW
Suite 1200
Washington, DC 20009-5715

Ph: 202.467.2900
Fax: 202.467.2910
www.APPAnet.org

Statement

Of the

AMERICAN PUBLIC POWER ASSOCIATION (APPA)

For the

HOUSE ENERGY AND AIR QUALITY SUBCOMMITTEE'S

Hearing regarding "Protecting the Electric Grid from Cyber-security Threats"

September 11, 2008

APPA appreciates the opportunity to provide the following testimony for the House Energy and Air Quality Subcommittee's hearing regarding "Protecting the Electric Grid from Cyber-security Threats." I am Susan Kelly, Vice President of Policy Analysis and General Counsel of APPA. With me is Allen Mosher, APPA's Senior Director of Reliability and Policy Analysis.

APPA represents the interests of more than 2,000 publicly-owned electric utility systems across the country, serving approximately 45 million Americans. APPA member utilities include state public power agencies and municipal electric utilities that serve some of the nation's largest cities. However, the vast majority of these publicly-owned electric utilities serve small and medium-sized communities in 49 states.

Introduction

Those of you who follow the electric utility industry closely know how rare it is that its trade associations speak with one voice on a federal energy policy issue. The associations in our industry represent a broad variety of stakeholder interests, including investor-owned, cooperatively-owned and publicly-owned utilities, independent generators, Canadian utilities, large industrial consumers, and state-public utility commissions. For very legitimate reasons, we usually have very different views on the policy issues facing our industry.

On the issue of protection of the electric bulk-power system from cybersecurity emergencies, however, we have come together. APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility

Commissioners, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group (associations) all support carefully crafted and specific legislation as the basis to deal with the discrete issue of cybersecurity emergencies. We understand the seriousness of the issue, and the need to deal with it. At the same time, we believe that such legislation must be carefully drawn and narrow in its application, to avoid disrupting the mandatory reliability regime that Congress has already required and the electric utility industry has implemented, with the oversight of the Federal Energy Regulatory Commission (FERC).

I have been asked by the Subcommittee to address the following subjects in my testimony: (a) whether the new federal emergency authority provided in the House discussion draft of legislation would be sufficient, but not excessive; (b) how that authority would fit with the current jurisdictional structure governing the bulk-power system; (c) whether all the governmental and industry actors involved and affected could be expected to respond, if such authority were invoked, in a timely and effective manner; (d) the degree to which the draft represents a consensus of views among stakeholders; (e) the nature of any remaining differences of views on specific provisions of the legislation; (f) the associations' recommended resolutions of those differences; (g) whether there are any important omissions in the draft; and (h) recommendations to the Subcommittee concerning its further actions with regard to this issue and the draft legislation. I will address each of these subjects in turn.

Whether the New Federal Emergency Authority Provided in the Draft Would Be Sufficient, but Not Excessive

The associations support the House discussion draft, **with the specific language options proposed by the associations**. This legislation is intended to fill a narrow gap in the

reliability standards regime that was established under section 215 of the Federal Power Act (FPA). Congress added this section to the FPA in section 1221 of the Energy Policy Act of 2005 (EPAct05). Section 215 was the result of a broad industry consensus in support of mandatory reliability standards. Under section 215, FERC has certified the North American Electric Reliability Corporation (NERC) as the nation's Electric Reliability Organization (ERO). The ERO is charged with the establishment and enforcement of mandatory standards for the bulk-power system intended to maintain its reliability, *i.e.*, to ensure that the lights stay on. NERC develops its reliability standards through a public and transparent standard-setting process that involves literally hundreds of volunteers from various sectors of the electric utility industry. FERC reviews these standards and either approves them or remands them to NERC for further consideration if it finds it cannot approve them. FERC can also order NERC to submit a proposed reliability standard or to revise an existing standard if FERC thinks such a standard is needed to assure reliability of the bulk-power system. NERC and its eight Regional Entities are charged with "front line" enforcement responsibilities for the resulting reliability standards, subject to FERC oversight. FERC also has its own independent standards enforcement authority. NERC's reliability standards apply to utilities in Canada and northern Mexico as well, although the legal and regulatory frameworks differ in those jurisdictions.

APPA believes this industry-based standards development and enforcement framework is working to ensure the reliable planning and operation of the bulk power system. To date, FERC has approved 94 mandatory reliability standards, while at the same time directing the ERO to consider many improvements to these standards. Critical Infrastructure Protection (CIP) is a case in point: so far, NERC has developed and FERC has approved nine CIP

standards. Based on FERC directives, NERC has also initiated a standards development project that will make further improvements to these standards.

Cybersecurity emergencies involving the bulk-power system, however, present a special case, for three reasons. First, cyber security emergencies by their nature entail protection against deliberate malicious attacks intended to disrupt system operations or cause other damaging consequences. In contrast, other reliability standards are generally designed to address random equipment failures, operator errors, and acts of God, such as hurricanes, with which the industry has many years of operational experience. Second, new, unforeseen threats could arise very quickly, leaving little time to react before attacks place reliable bulk-power system operation at risk. The swift pace of changes in information technology increases such risks. While NERC does have expedited standard development procedures in place, and is considering further improvements to those procedures, at present, there is a timeliness issue in such special cases. Third, there is a need for confidentiality regarding the nature of the threat, the risks that it poses to reliable operations, and the measures to be taken to address it, at least until such time as the initial measures can be implemented. NERC is currently considering how its standard-setting process can be revamped to deal with such confidentiality issues, while still getting the industry input needed to ensure that standards are broadly supported and resolve the problem in the most effective manner, without unintended consequences for other aspects of system operations. At this time, however, confidentiality is an issue in such special cases.

For these reasons, the associations support specific legislation that would serve as an appropriate basis to address the unique circumstances that cybersecurity emergencies raise, and no more. Any such legislation should be narrowly drawn to address the identified

problem. In particular, Congress should take care not to undermine the section 215-based reliability standards-setting process. While the regime is still relatively new, it has already brought salutary changes to our industry in the area of reliability. Users, owners and operators of the bulk-power system subject to the regime have made substantial progress in implementing the new reliability standards, including the CIP standards. This mandatory standards regime needs to be allowed to continue to develop and mature.

How the Authority Would Fit with the Current Jurisdictional Structure Governing the Bulk-Power System

The House discussion draft has been crafted to dovetail with the current jurisdictional structure governing the bulk-power system. First, like FPA section 215, its applicability is limited to "users, owners and operators" of the bulk-power system. That term has been defined in section 215(a)(1) as follows:

> The term 'bulk-power system' means—(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.[[1]]

The practical application of the term "users, owners and operators of the bulk-power system" has been developed in the course of NERC's implementation of the mandatory reliability standards I previously discussed. NERC has a Compliance Registry that lists those users, owners and operators of the bulk-power system that must comply with at least some portion of NERC's reliability standards. Those listed in the Compliance Registry are included based on Compliance Registry Criteria that have been developed by industry stakeholders and NERC, and subsequently approved by FERC. Retail customers and local distribution

[1] Note also that FPA section 215(k) provides that "[t]he provisions of this section do not apply to Alaska or Hawaii."

facilities, small generators, and small utilities are generally excluded from this reliability regime.

In the view of the electric utility industry and its State regulators, it is best to limit the new cybersecurity legislation to this same universe of facilities and entities. To do otherwise (for example, to expand the reach of the legislation to encompass local distribution facilities) would raise jurisdictional and implementation issues that could greatly complicate consideration of legislation on this issue. As members of the Subcommittee are well aware, local distribution facilities in the States are regulated by State regulatory commissions, which are responsible for ensuring that retail utility service is provided safely and reliably within their respective jurisdictions. As Congress recognized in FPA section 215(i)(3), the authority of the States to regulate the reliability of local distribution networks and service should be preserved, with FERC's regulatory authority focused on the operations of the bulk-power system.

For these reasons, the industry believes that the jurisdictional lines drawn in the House discussion draft are the proper ones.

Whether the Governmental and Industry Actors Involved and Affected Could Be Expected to Respond, if Such Authority Were Invoked, in a Timely and Effective Manner

The House discussion draft has been fashioned to allow FERC to address cybersecurity emergencies as swiftly as possible, while still providing for appropriate consultation with governmental authorities (including Canadian and Mexican authorities) and affected users, owners and operators of the bulk-power system in the United States. The industry itself is proceeding up the learning curve on responding to notices of cybersecurity threats, having

learned a number of lessons through its response to the Aurora vulnerability in 2007. Since I am not an expert in this area, I will defer on this issue to the other industry witnesses appearing before the Subcommittee.

The Degree to Which the House Discussion Draft Represents a Consensus of Views Among Stakeholders

As I noted at the outset of my testimony, APPA and the other associations support carefully crafted legislation to address cybersecurity emergencies. While individual associations may have differed over certain specifics of the proposed legislation at the outset, intense negotiations among the associations themselves and jointly with FERC over the last several weeks have resulted in a consensus association position on legislation.

The Nature of Any Remaining Differences of Views on Specific Provisions of the Legislation and Your Recommended Resolutions of those Differences

The associations negotiated at length with representatives of FERC regarding the earlier version of the House discussion draft. We were able to reach closure on many issues, and we thank the FERC staff for the constructive and positive attitude it maintained during these negotiations. Nonetheless, we were unable to reach closure on three issues, as reflected in the recently released version of the House discussion draft. These three areas are:

- Definition of "Cyber security Threat." The industry and FERC agreed on most elements of this definition, but differ in two respects. First, we believe that there should be a *substantial* likelihood of a malicious act for the federal government to conclude that there is a cybersecurity threat that would trigger the need for

emergency action. FERC would prefer a simple "likelihood" of such an act. Second, we believe there should be both a substantial likelihood of a malicious act *and* a substantial possibility of disruption to the operation of the system in the event of such an act, to constitute a "cybersecurity threat." FERC would prefer the definition to be phrased in the disjunctive ("or"). The associations believe their preferred definition limits the legislation appropriately to cybersecurity emergencies – meaning threats that have a substantial likelihood of happening and that could substantially disrupt the reliable operation of the bulk-power system if they do happen.

- Inclusion of "Other National Security Threats." FERC would prefer to expand the legislation to include "other national security threats" in addition to cybersecurity threats. The associations believe that other government entities, both state and federal, have more direct responsibilities in the general area of national security. Moreover, this additional authority is quite vague in its wording and hence potentially all-encompassing in nature, which in and of itself raises substantial concerns. Finally, including such language could spark an intense discussion that could slow down the legislation considerably. For all these reasons, the associations do not favor including it.

- "Sunset" of Interim Measures that FERC Enacts under Subsection (b). The industry and FERC negotiated at length regarding the "sunset" provision of subsection (d) (entitled "Discontinuance"). We were able to reach closure on almost all of the issues, but one remains outstanding. The associations believe that the sunset provision in subsection (d)(4) should apply to both interim measures FERC implements under subsection (b) and emergency measures it implements under

subsection (c). We believe this should be the case because we regard measures and orders under both sections as either being limited in time by their nature, or to be replaced by reliability standards NERC develops using section 215 procedures. FERC, however, does not accede to this position as to actions it takes under subsection (b).

While the associations could not reach closure with FERC on these three issues, this should not overshadow the substantial progress we did make in the negotiations regarding draft legislation. For all of our associations and the federal regulator to reach closure on the issues this legislation raises, save these three, is noteworthy.

Whether there Are Any Important Omissions in the Draft

The associations generally believe that the House discussion draft, with acceptance of the associations' proposed language options, would cover the important areas that need to be covered. For the reasons stated above, others (and, in particular, FERC) may disagree with the associations' view on this issue.

Recommendations to the Subcommittee Concerning Its Further Actions with Regard to This Issue and the Draft Legislation

The associations support narrowly focused legislation as a basis to address the issue of cybersecurity emergencies involving the bulk-power system. We strongly urge Congress to retain the carefully crafted legislative language reflected in the House discussion draft, with the proposed language options that the associations support, as the process moves forward.

Conclusion

Thank you for the opportunity to present APPA's views on the House discussion draft. We look forward to continuing to work with the Subcommittee on this important issue and are available to provide any further assistance.

Mr. BOUCHER. Thank you very much, Ms. Kelly. Mr. Naumann.

STATEMENT OF STEVEN T. NAUMANN, VICE PRESIDENT, WHOLESALE MARKET DEVELOPMENT, GOVERNMENT AND ENVIRONMENTAL AFFAIRS AND PUBLIC POLICY, EXELON CORPORATION

Mr. NAUMANN. Thank you, Mr. Chairman, members of the subcommittee. My name is Steven Naumann. I am Vice President for Wholesale Market Development for Exelon Corporation. I serve as Vice Chairman of the Members Representative Committee of NERC. I am also accompanied by Mr. Dan Hill, Exelon Senior Vice President and Chief Information Officer. I appreciate the opportunity to testify about protecting the electric grid from cybersecurity threats.

I am appearing today on behalf of the Edison Electric Institute and the Electric Power Supply Association, and Exelon is a member of both these groups. My testimony focuses primarily on the nature of cybersecurity threats to the bulk power electric system and the efforts of electric utilities to respond to those threats, but it will also touch on proposed legislation before the subcommittee.

I want to start, however, by assuring the subcommittee that Exelon and other electric utilities take cybersecurity very seriously. Electric utilities routinely monitor for and detect electronic probing of their systems from a variety of sources, confirming the likelihood of real cybersecurity threats. However utilities and other private sector entities are at a disadvantage in assessing the degree and the urgency of possible or perceived cyber threats because of their limited access to intelligence possessed only by the government.

Many cybersecurity issues are already being addressed under current law. Critical infrastructure protection standards have been implemented under section 215 of the Federal Power Act, which provide for mandatory and enforceable reliability rules.

However, the current reliability regime has limitations in its ability to be responsive to emergencies requiring immediate, focused, and confidential actions. Therefore it is appropriate for Congress to provide FERC with explicit authority to address cybersecurity in certain emergency situations.

Any new FERC authority should be complementary to the existing authorities under section 215 of the Federal Power Act, which rely on the industry expertise as the foundation for developing reliability standards. Legislation should clarify the respective roles, responsibilities, and procedures of the Federal government and of industry; be narrowly tailored to deal with real emergencies; and promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures.

The scope of damages that could result from a cybersecurity threat depends on the details of any particular incident, but a carefully planned cyber attack could have potentially serious consequences. In mitigating a particular cybersecurity vulnerability, electric utilities must also consider the potential consequences caused by any mitigation measure on safe and reliable utility operations.

For these reasons, for ensuring the cybersecurity of the bulk power system, the best framework is one that utilizes the respec-

tive strengths of both the government and the electric companies. It is critically important that as much as possible, any cybersecurity framework provide for ongoing consultation and sharing of information between government agencies and utilities to the extent possible.

In conclusion, I want to reassure the subcommittee that owners, operators, and users of the bulk power system take cybersecurity very seriously. We are actively engaged in addressing threats as they arise, and in employing specific strategies that make every reasonable effort to protect our cyber infrastructures and mitigate the risks of cyber threats.

As the industry relies increasingly on electronic and computerized devices and connections and the nature of cyber threats continually evolves and becomes more complex, cybersecurity will remain a constant challenge. But we believe we are up to the task of building on the industry's historical and deep-rooted commitment to maintaining system reliability.

I appreciate the opportunity to appear today and would be happy to answer any questions. Thank you.

[The prepared statement of Mr. Naumann follows:]

EDISON ELECTRIC INSTITUTE

epsa
Electric Power Supply Association

Statement of
Steven T. Naumann
Vice President, Wholesale Market Development
Exelon Corporation

On Behalf of
Edison Electric Institute
and
Electric Power Supply Association

Before the
Subcommittee on Energy and Air Quality
Committee on Energy and Commerce
U.S. House of Representatives

September 11, 2008

Executive Summary
Statement of Steven T. Naumann
Exelon Corporation
On Behalf of
Edison Electric Institute and Electric Power Supply Association

Electric utilities take cyber security very seriously and are actively engaged in identifying and employing strategies to protect our cyber infrastructure and mitigate the risks of cyber threats.

While many cyber security issues are already being addressed under current law, it is appropriate to provide FERC with explicit statutory authority to address cyber security in certain emergency situations. Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation for developing reliability standards. Any legislation should clarify the respective roles, responsibilities, and procedures of the federal government and the industry; be narrowly tailored to deal with real emergencies; and promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures.

Electric utilities routinely monitor for—and detect—electronic probing of their systems from a variety of sources, confirming the likelihood of real cyber security threats. However, utilities and other private sector entities are at a disadvantage in assessing the degree and urgency of possible or perceived cyber threats because of their limited access to intelligence information possessed only by the government. Electric utilities *are* in a unique position to understand the consequences of a potential malicious act on their systems as well as proposed preventive and mitigation actions. Therefore, the optimal approach to ensuring the cyber security of the bulk power system utilizes the respective strengths of both government intelligence specialists and electric utilities, and provides for ongoing consultation and sharing of information between government agencies and utilities.

The scope of the damages that could result from a cyber security threat depends on the details of any particular incident. Because utility operations vary greatly, it is difficult to generalize about the impacts of a particular threat, or about costs and time required to mitigate a threat or vulnerability. A carefully planned cyber attack could potentially have serious consequences. In mitigating a particular cyber security vulnerability, electric utilities must also consider the potential consequences caused by any mitigation measures on safe and reliable utility operations.

As the electric utility industry relies increasingly on digital information and controls, it must work closely with vendors and manufacturers to ensure that cyber security protections are incorporated into devices as much as possible. It is equally critical that the architecture underpinning cyber security solutions for the grid and the architecture being developed for smart grid solutions are synchronized and compatible so that the smart grid solutions and the great benefits they will provide will be implemented in a secure fashion.

Mr. Chairman and Members of the Subcommittee:

My name is Steve Naumann, and I am Vice President for Wholesale Market Development for Exelon Corporation. I also serve as Vice Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC). I am accompanied today by Dan Hill, Exelon's Senior Vice President and Chief Information Officer, who has day-to-day responsibility for cyber security issues in our company. I appreciate your invitation to appear today and the opportunity to testify about protecting the electric grid from cyber security threats.

Exelon is a holding company headquartered in Chicago. Our retail utilities, ComEd in Chicago and PECO in Philadelphia, serve 5.4 million customers, or about 12 million people – more than any other company. Our generation subsidiary, Exelon Generation, owns or controls approximately 30,000 MW of generating facilities, including fossil, hydro, nuclear and renewable facilities. Our nuclear fleet consists of 17 reactors; it is the largest in the nation and the third largest in the world.

I am appearing today on behalf of the Edison Electric Institute (EEI), of which Exelon is a member. EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members worldwide. EEI's U.S. members serve 95% of the ultimate customers in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry.

I am also testifying today on behalf of the Electric Power Supply Association (EPSA), of which Exelon is also a member. EPSA is the national trade association representing competitive power suppliers, including generators and marketers.

My testimony focuses on the nature of cyber security threats to the bulk power electric system and the efforts of electric utilities to respond to those threats. I want to reassure the Subcommittee that electric utilities and other owners, operators, and users of the bulk power system take cyber security very seriously. We are actively engaged in addressing cyber security threats as they arise and in employing specific strategies that make every reasonable effort to protect our cyber infrastructure and mitigate the risks of cyber threats. As the industry relies increasingly on electronic and computerized devices and connections, and the nature of cyber threats continually evolves and becomes more complex, cyber security will remain a constant challenge for the industry. But we believe we are up to the task, building on our industry's historical and deep-rooted commitment to maintaining system reliability.

Legislation Generally

I agree with other witnesses that it is appropriate for Congress to consider legislation providing the Federal Energy Regulatory Commission (FERC) new authority to address emergency cyber security threats. I want to emphasize, however, that current law already provides the means to address many cyber security issues in the electric industry. Section 215 of the Federal Power Act, which this Subcommittee helped develop and which was enacted by Congress as part of the Energy Policy Act of 2005, provides for mandatory and enforceable electric reliability rules, specifically including rules to address cyber security, under FERC oversight.

The basic construct of the relationship between FERC and NERC in developing and enforcing reliability rules is sound. In summary, NERC, using a well-defined stakeholder process that leverages the vast technical expertise of the owners, users, and operators of the North American electric grid, develops reliability standards, which are then submitted to FERC

for review and approval. Once approved by FERC, these standards are legally binding and enforceable in the United States.

I suggest the question on which the Subcommittee should focus is, "What additional authority should be provided to FERC in order to promote clarity and focus in response to emergency situations?" Legislation in this area should complement, not supplant, the mandatory reliability regime already established under Section 215, and any new FERC authority should be appropriately narrow and focused only on unique problems that cannot be addressed under Section 215. The Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation.

Any cyber security legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. Consultation is critical to improving cyber security. To the extent practicable, the construct provided by existing law should be replicated for imminent cyber security threats.

Specific Issues Related to Risks and Mitigation

The following comments address the specific issues raised by the Subcommittee in its invitation to testify:

- **The degree and urgency of the perceived risks to the bulk power system and those it serves and the evidence that such risks are real based on experience (limited to unclassified information).**

Because electric utilities and other companies routinely monitor for—and through such monitoring detect—electronic probing of our systems from a variety of sources, we must assume there is a real cyber security threat that all private sector entities face, including utilities. There is other generally available evidence that cyber security threats are real in the form of publicized events regarding exploitation of cyber security vulnerabilities, but it is important to note that to my knowledge no documented exploitation of electric utility systems affecting the North American bulk power system has occurred to date.

Fundamentally, however, the private sector is at a disadvantage in assessing the degree and urgency of possible or perceived cyber threats because of our limited access to intelligence information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems operate. Owners, users, and operators of the bulk power system are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such an exploitation. Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and electric utilities in ensuring the cyber security of the nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for ongoing consultation and sharing of information between government agencies and utilities.

- **The extent to which the utility industry and other key participants in grid operations are or are not already prepared or currently undertaking protective measures.**

Exelon, like other utilities, takes cyber security extremely seriously. We are addressing the risks we know about through a "defense-in-depth" strategy while appropriately balancing considerations of potential consequences. This defense-in-depth strategy includes preventive, monitoring and detective measures to ensure the security of our systems. For example, we perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform us about whether our preventive strategies are working so that we can enhance our protection as technologies and capabilities evolve. Penetration testing also allows us to practice and enhance our monitoring capabilities.

Exelon responded to the "Aurora" vulnerability after learning about it through our nuclear business unit and then through an advisory that was sent to the electric industry by NERC in the summer of 2007. "Aurora" is a government laboratory's code name for a vulnerability that could allow an unauthorized person who gained remote access to certain electronic devices to cause damage to other pieces of equipment. We have taken the recommended actions to mitigate the vulnerability. While I do not have firsthand knowledge of what other utilities have done, based on my knowledge of the industry and conversations with my peers at other utilities, I believe other similarly situated utilities have also taken the risk seriously and have responded in an appropriate fashion.

- **The scope of damages that could be inflicted if adequate protective measures are not taken.**

Obviously, the scope of the damages that could result from a cyber security threat depends on the details of any particular incident. A carefully planned cyber attack could potentially have serious consequences. This is why Exelon and other electric utilities take cyber security very seriously and have implemented strong cyber security programs to mitigate these risks.

Regardless of the scope of damages that any particular cyber security threat might inflict, owners, users, and operators of the bulk power system must also consider the potential consequences caused by any mitigation measures, such as potential impact to safe and reliable ongoing utility operations and service to electricity customers. Examples might include slower responses during emergency operations, longer times for restoration of outages and disruption of business operations dependent on Internet access. That is why each situation requires careful consultation with owners, users, and operators to ensure that a measure aimed at protecting the grid from a malicious cyber attack does not instead cause other unintended and harmful consequences.

- **The costs and time required for mitigation of such risks.**

Many issues that may affect the overall security of the grid are not emergencies and thus do not need to be handled within hours or even days. Information about cyber security vulnerabilities and attempts to exploit those vulnerabilities is shared with electric industry owners, users, and operators through a number of channels every day. Federal agencies that communicate threat information to the private sector, such as the United States Computer Emergency Readiness Team (US-CERT), as well as cyber security hardware and software vendors, classify vulnerabilities in terms of the generalized risk to systems. Factors such as the

seriousness of consequences of a successful attack, the sophistication required to conduct the attack, and how widely used the potentially affected assets are within an industry are used to rank vulnerabilities as "high", "medium", or "low" risk. Many, if not most, of the vulnerabilities the electric industry learns about are ranked as being a relatively "low" risk.

Furthermore, every utility operates different equipment in different environments, making it difficult to offer generalizations about the impacts to the bulk power system or costs and time required to mitigate any particular threat or vulnerability. This complexity underscores the importance of consultation with owners, users, and operators to ensure that any mitigation that may be required appropriately considers these factors to ensure an efficient and effective outcome. For the foregoing reasons, any new legislation giving FERC additional statutory authority should be limited to true emergency situations – as declared by the President or his designee.

- **How protection from cyber security breaches can be assured even as the electricity industry continues to evolve toward "smart grid" capabilities including greater use of digital information and controls.**

As grid technologies continue to evolve, they inevitably will include greater use of digital controls. Congress recognized the potential cyber security vulnerabilities, as well as benefits, that could result from greater digitalization of the grid when it directed the Department of Energy to study these issues in Section 1309 of the Energy Independence and Security Act of 2007.

As new "smart grid" technologies are developed, it will be imperative for the industry to work closely with vendors and manufacturers to ensure they understand that cyber security is essential so that cyber security protections are incorporated into devices as much as possible.

It is equally critical that the architecture underpinning cyber security solutions for the grid and the architecture being developed for smart grid solutions are synchronized and compatible so that the smart grid solutions and the great benefits they will provide will be implemented in a secure fashion. With smart grid solutions in the early stages of development, opportunities exist to ensure this compatibility.

- **Conclusion**

While many cyber security issues are already being addressed under current law, we believe it is appropriate to provide FERC with explicit statutory authority to address cyber security in a situation deemed sufficiently serious to require a Presidential declaration of emergency. In such a situation, the legislation should clarify the respective roles, responsibilities, and procedures of the federal government and the industry, including those for handling confidential information, to facilitate an expeditious response.

Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation for developing reliability standards. Any new authority should also be narrowly tailored to deal with real emergencies; overly broad authority would undermine the collaborative framework that is needed to further enhance security.

Promoting clearly defined roles and responsibilities, as well as ongoing consultation and sharing of information between government and the private sector, is the best approach to improving cyber security. Each cyber security situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the bulk power system.

Exelon and other electric utilities remain fully committed to working with the government and industry partners to increase cyber security.

I appreciate the opportunity to appear today and would be happy to answer any questions.

Exelon

Exelon Corporation
P. O. Box 805398
Chicago, IL 60680-5398

October 7, 2008

The Honorable Rick Boucher
Chairman
Subcommittee on Energy and Air Quality
Committee on Energy and Commerce
United States House of Representatives
2187 Rayburn HOB
Washington, DC 20515

Dear Chairman Boucher:

It was an honor to testify on behalf of the Edison Electric Institute and the Electric Power Supply Association at the Subcommittee's hearing entitled "Protecting the Electric Grid from Cyber-Security Threats" on September 11, 2008. During the course of that hearing, I was asked what my company's costs were for complying with the North American Electric Reliability Corporation June 21, 2007 communication, also referred to as the Aurora Advisory. I did not have an answer at that time, but, pursuant to your request, have since canvassed Exelon Corporation's various operating companies to ascertain the costs that were incurred in complying with the Aurora Advisory.

Our review of the costs incurred by the Exelon companies - Commonwealth Edison Company, Exelon Generation Company, and PECO Energy - indicates that compliance with the Aurora Advisory resulted in a total cost to Exelon of approximately $1.2 million. Those costs reflect both internal and external costs though most of the costs reflected in the aforementioned figure were internal. I should note that Exelon's mitigation measures in the Aurora Advisory did not require costly equipment replacement. While we are able to calculate the costs stemming from Aurora, the costs of complying with future advisories or standards might be quite different depending on the specific circumstances. I should also note that our costs may or may not be representative of what was incurred by others in our industry given our company's somewhat unique portfolio of assets.

I commend you on your efforts on this important matter. As the Subcommittee continues its work on this issue, please do not hesitate to call on me if you have any further questions.

Sincerely,

Steven T. Naumann
Vice President, Wholesale Market Development

cc: The Honorable Fred Upton
Ranking Member

Mr. BOUCHER. Thank you very much, Mr. Naumann. Mr. Lawson.

STATEMENT OF BARRY R. LAWSON, MANAGER, POWER DELIVERY, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

Mr. LAWSON. Chairman Boucher, Ranking Member Upton, and members of the subcommittee, thank you for the opportunity to testify today on cybersecurity issues and their potential impacts on the bulk power system. My name is Barry Lawson, and I am the manager of power delivery for the National Rural Electric Cooperative Association. NRECA is a trade association consisting of nearly 1,000 cooperatives, providing electricity to 41 million consumers in 47 States.

One of my primary areas of responsibility at NRECA is reliability, including cybersecurity. NRECA and its members understand the importance of cybersecurity. To arrive at the draft bill before you today, NRECA has worked closely with its industry counterparts and with FERC and NERC.

NRECA commends FERC under Chairman Kelliher's leadership for its proactive outreach on the topics we are discussing today. Provisions in this draft bill can provide swift, effective emergency protection to the bulk power system in those limited circumstances when NERC cannot. NRECA supports the House discussion draft with the specific language options proposed by the associations.

NRECA has been actively engaged with NERC from its origin over 35 years ago, to its transition into the industry ERO and as it issues reliability standards, including the cybersecurity standards FERC approved earlier this year.

In January 2008, I began a 2-year chairmanship of the NERC critical infrastructure protection committee. The CIPC is a NERC standing committee that advises the NERC board of trustees on issues related to critical infrastructure protection including cybersecurity. My position on the CIPC requires me to interact with NERC, DOE, and DHS staff on an ongoing basis and contributes to the viewpoints I will share with you today.

As both a participant in NERC and an interested observer of its role as the ERO, NRECA believes that the self-regulatory model is the best means of maintaining a strong, reliable bulk power system. The model recognizes that the electric industry addresses events and threats every day, including those posed by natural disasters, vandalism, and equipment failures.

Last fall, many Members of Congress and the public were introduced to cybersecurity when news outlets ran a story and video showing a small electric generator that was damaged during a test. The news report said a government lab had demonstrated that computer hackers could cause physical damage to equipment through cyber means. The government labeled this vulnerability Aurora.

Today, almost no one outside the intelligence community has been able to examine the technical and engineering details of the Aurora vulnerability. Key information about the vulnerability is still classified.

Members of the NERC CIPC first received limited, unclassified information about the Aurora vulnerability from DHS in March of 2007. We were strictly prohibited from sharing this information, meaning I could not inform member cooperatives.

In June 2007, DHS placed limited information and mitigation measures into a document that NERC utilized as an industry advisory. Although these measures did not reveal specifics about the vulnerability, cooperatives and other utilities that own or operate bulk power system facilities used their collective expertise to implement the measures on their individual systems.

Aurora demonstrated the need for utilities to receive more timely and detailed information from intelligence sources about threats and vulnerabilities and their engineering, cyber, and mechanical implications.

Under the existing rules and procedures created by NERC and approved by FERC, NERC can deal with a wide range of cyber threats. NERC's standards development process can sometimes be lengthy to accommodate the highly technical nature of the subject matter. But it can also be shortened when expediency demands.

NERC has two special procedures for developing standards more quickly. The urgent action process was developed to approve standards within a few months, and the emergency action process was developed to approve standards within a few weeks. Both processes should be used whenever needed for the expedient development of reliability standards, including those related to cybersecurity.

As Mr. Sergel explained to you, NERC recently wrote its board of trustees and industry stakeholders to explain changes and improvements it plans regarding its focus on cybersecurity. This NERC initiative is critically important to the reliability of the bulk power system, and we support these efforts.

NRECA is working closely with its counterparts across the industry and agrees there is potential for some cyber threats and vulnerabilities so imminent and substantial that even revised and strengthened NERC procedures cannot assure the timely distribution of information and direction to industry to effectuate an adequate industry response to protect the bulk power system.

In those limited circumstances when the President of the United States has determined emergency action is warranted, FERC should be able, after consulting industry and government authorities in Canada and Mexico to issue, orders addressing the emergency.

In conclusion, NRECA supports the House discussion draft with the specific language options proposed by the associations. Like our industry counterparts, NRECA is prepared to assist the subcommittee and full committee with advancing this legislation. NRECA also looks forward to continued cooperation with FERC.

I am happy to answer any questions you have.

[The prepared statement of Mr. Lawson follows:]

Statement of NRECA to the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Energy and Air Quality

Hearing on: Protecting the Electric Grid from Cyber-Security Threats

September 11, 2008

4301 Wilson Boulevard
Arlington VA 22203
www.nreca.coop

Executive Summary of Testimony

NRECA has worked closely with its industry counterparts, and with FERC and NERC to arrive at the legislation before you today. All parties in these discussions and negotiations recognized the seriousness of the security issues facing our nation and each worked diligently to craft legislative language that can provide swift, effective emergency protection to the bulk power system in those limited circumstances when the ERO cannot. NRECA supports the House discussion draft, with the specific language options proposed by the associations.

NRECA worked with Congress, the Federal Energy Regulatory Commission (FERC) and its industry counterparts to ensure that the 2005 Energy Policy Act (EPAct) contained strong and effective reliability provisions. NRECA has actively participated in the formation and development of the industry reliability self-regulatory organization, the North American Electric Reliability Corporation (NERC), in its role as the Electric Reliability Organization (ERO). NRECA has also been very engaged in the creation of NERC's initial reliability standards, including the cyber-security standards that FERC approved earlier this year.

For the last several years NRECA has worked closely with its electric cooperative membership on reliability issues, including those related to cyber-security. In 2005 NRECA held a series of workshops for its members on numerous cyber-security issues, including defense-in-depth practices, disaster and business continuity planning and other industry best practices for protecting cyber networks. Since June 2007 NRECA worked closely with NERC to distribute the "Aurora" mitigation measures to electric cooperatives. We also provided support to our members to help them understand the importance of these issues and the need for them to take the steps included in the mitigation measures document.

As both a participant in NERC and an interested observer of its role as the ERO, NRECA believes that the self-regulatory model is the best means of maintaining a strong, reliable bulk power system. The self-regulatory model recognizes that the electric industry overcomes some level of threat every day, ranging from those posed by inclement weather or other natural events,

to vandalism and equipment failures. The NERC structure has increased the industry's capacity to respond to a wider variety of intentional and accidental threats. Working together, FERC, NERC and industry will continue to improve an already exemplary record of maintaining and protecting the nation's electric infrastructure and continuing its high level of reliability.

For the overwhelming majority of identified threats and vulnerabilities, existing industry and NERC procedures provide the necessary response for the continued reliability of the bulk power system. There are potential improvements to ERO procedures that can increase the amount and variety of threats and vulnerabilities the industry can handle through the self-regulatory process and NERC is currently working on these issues.

However, in an age of increasing reliance on computer and web-based controls in the electric transmission and generation infrastructure, it is conceivable that some threats may be so severe and imminent that the self-regulatory model may not sufficiently protect the bulk power system. In those limited circumstances, it is appropriate to provide, in legislation, a back-stop, emergency authority which extends until the threat is mitigated, ends or is reduced to such a level that the ERO's procedures and standards can once again meet the challenge.

Introduction

Chairman Boucher, Ranking Member Upton and members of the Subcommittee, thank you for the opportunity to testify today on cyber-security issues and their potential impacts on the bulk power system.

My name is Barry Lawson, and I am the Manager, Power Delivery for the National Rural Electric Cooperative Association (NRECA). One of my primary areas of responsibility at NRECA is reliability, including those issues related to cyber-security. NRECA is a trade association consisting of nearly 1,000 cooperatives providing electricity to 41 million consumers in 47 states. As member-owned, not-for-profit organizations, cooperatives have an obligation to provide a reliable supply of electricity to all consumers in our service areas at the lowest possible price. Cooperatives serve primarily the more sparsely populated parts of our nation but cover roughly 75 percent of the nation's land mass and maintain 42 percent of the nation's electric distribution lines.

Along with many colleagues, including some of those on the panel today, I continue to work closely on reliability and cyber-security issues, with electric cooperatives, other electricity industry sectors, FERC and NERC. NRECA commends FERC, under Chairman Kelliher's leadership for its proactive outreach on the topics we are discussing today.

In January 2008, on behalf of NRECA and its members, I began a two-year chairmanship of the NERC Critical Infrastructure Protection Committee (CIPC). The CIPC is a NERC standing committee that advises the NERC Board of Trustees on issues related to critical infrastructure protection, including cyber-security. My position on the CIPC requires me to interact with NERC, Department of Energy (DOE) and Department

of Homeland Security (DHS) staff on an ongoing basis and contributes to the viewpoints I will share with you today.

Industry Cooperation in Response to the "Aurora" Vulnerability

Last fall, many members of Congress and the public at large were introduced to the concept of cyber-security when news outlets ran a story and video showing a small electric generator that was damaged during a test. The news reports said a government lab had demonstrated that computer hackers could cause physical damage to equipment through cyber means. The government labeled this vulnerability "Aurora." Today, almost no one outside the intelligence community knows what the "Aurora" vulnerability actually means from a technical or engineering standpoint. Information about the vulnerability is still classified.

The "Aurora" example and the industry's response to it highlight concepts I will discuss in my testimony today:

- NERC already has many existing procedures and reliability standards to meet ongoing threats and vulnerabilities.
- The self-regulatory structure and level of industry investment in the ERO provide the means to improve and revise existing procedures and reliability standards to address additional threats and vulnerabilities.

As a member of the NERC CIPC, I first received information about the "Aurora" vulnerability in March 2007. DHS gave CIPC members limited information about the vulnerability but strictly prohibited us from sharing that information with others even though the unclassified information provided would have been beneficial for others to receive. I could not inform key staff at NRECA or, more importantly, any of the NRECA

member cooperatives. Several months later DHS then placed limited information into a document that NERC relied on to distribute as mitigation measures to the industry on June 21, 2007. It was at that time I was first permitted to share the information with key staff at NRECA and NRECA member cooperatives. Although the mitigation measures did not reveal the specific technical or cyber vulnerability the actions would protect against, cooperatives, and other utilities that own or operate bulk power system facilities, used their collective expertise to implement the measures on their individual systems to mitigate the Aurora vulnerability.

NERC Currently Equipped to Handle Many Threats and Vulnerabilities

The Subcommittee should be aware of the procedures and standards used to respond to "Aurora." These existing NERC processes allow NERC and the industry to assess a wide variety of threats and vulnerabilities and then devise and implement effective industry responses.

Under the existing rules and procedures created by NERC and approved by FERC, NERC has the capability to deal with a wide range of cyber threats. For issues that can be addressed with longer-term solutions, NERC and industry develop standards as prescribed by FERC under Section 215 of the Federal Power Act as passed in Section 1221 of EPAct. NERC's standards development process is designed to develop mandatory reliability standards for users, owners and operators of the bulk power system. This process can sometimes be lengthy to accommodate the highly technical nature of the subject matter, but it can also be shortened if conditions require expediency. NERC's normal process can take a number of months to longer than a year to develop a standard. However, NERC also has in its Reliability Standards Development Procedure, as

approved by FERC, two special procedures for developing standards more quickly. The Urgent Action process was developed to approve standards within a few months and the Emergency Action process was developed to approve standards within a few weeks if necessary. The Urgent and Emergency Action processes should be used to the extent they are needed for the expedient development of reliability standards, including those related to cyber security.

In addition, NERC has in its Rules of Procedure, as approved by FERC, the ability to distribute advisories on topics that are important for industry to address. There are three levels of advisories, including the most critical advisory level entitled "Essential Action." We strongly support NERC's use of the advisory tool to quickly – within hours or days – distribute important information to the industry for action.

Improvements to Existing NERC Procedures Can Help Meet Additional Threats and Vulnerabilities

On July 7, 2008, NERC wrote its Board of Trustees and industry stakeholders to explain the changes and improvements it plans to make regarding its focus on cyber-security. These ongoing NERC efforts to improve its ability to respond quickly and efficiently to cyber-security threats and vulnerabilities are critically important to reliability of the bulk power system.

I want to highlight for you three specific efforts by NERC. First, NERC has recently hired a Chief Security Officer (CSO), who will be responsible for coordinating cyber-security matters across all NERC activities. We look forward to working closely with the new CSO. Second, we support NERC's plan to develop an Emergency/Crisis

standards setting process for cyber-security. Finally, we agree with NERC that there is a need to develop closer coordination with government on cyber-security issues.

Substantial and Imminent Threats May Require Exercise of Emergency Authority

NRECA, working closely with its counterparts across the electric industry, agrees there is potential for some threats and vulnerabilities so imminent and substantial that even revised and strengthened NERC procedures cannot assure the timely distribution of information and direction to industry to effectuate an adequate industry response to protect the bulk power system.

In those limited circumstances, when the President of the United States has determined that emergency action is warranted, FERC should have the authority to issue orders, after consultation with the industry and relevant governmental authorities in Canada and Mexico, that directly address the vulnerability and/or threat and the necessary mitigation actions needed to protect the bulk power system.

Answers to Specific Subcommittee Questions

In requesting my testimony, you asked me to address several specific points about the nature and urgency of the threat to the electric system from cyber-security breaches. NRECA is in agreement with the points in the Edison Electric Institute's (EEI) testimony regarding operational issues. My answers are based on my own experience as a member of the CIPC and a resource for operational and cyber experts working on-the-ground at cooperatives.

(a) The degree and urgency of the perceived risks to the bulk power system and those it serves and (b) the evidence that such risks are real based on experience (limited to unclassified information).

The electric industry has decades of experience in assessing a wide variety of threats to critical infrastructure assets. Electric utilities have focused on cyber threats increasingly over time, in proportion to the increasing use of automated components in generation and transmission of electricity.

It is important to note that each utility has a mix of older and newer equipment. Many parts of the bulk power system operating today still rely on mechanical components that are not programmable and these older assets in many cases are not vulnerable to cyber threats as is some of the newer equipment.

Since 2001, I have been involved in critical infrastructure protection issues, including those related to cyber. I can tell you based on my own experience that the cooperative industry takes cyber threats and vulnerabilities very seriously. However, to my knowledge, including that gained serving on the CIPC for six years, there are no documented cases of successful attempts to damage the North American bulk power system through cyber channels.

(c) The extent to which the utility industry and other key participants in grid operations are or are not already prepared or currently undertaking protective measures.

My job at NRECA requires me to assist electric cooperatives that own or operate bulk power system assets in complying with FERC's mandatory reliability standards. Based on workshops, presentations and in regular interactions with our membership, I believe cooperatives are addressing known cyber threats and vulnerabilities.

(d) The scope of damages that could be inflicted if adequate protective measures are not taken and (e) the costs and time required for mitigation of such risks.

The scope of potential damages is as wide as the scope of potential events. If utilities receive more timely and detailed information from intelligence sources about threats and vulnerabilities and their engineering, cyber and mechanical implications, utilities can then better assess the mitigation steps needed and balance those with the potential likelihood of a successful attack. Utilities must also consider the reliability impacts of any action concerning their generation and transmission assets, including those posed by mitigation measures.

(f) How protection from cyber-security breaches can be assured even as the electricity industry continues to evolve toward "smart grid" capabilities including greater use of digital information and controls.

Like our industry counterparts, cooperatives are moving steadily toward smart grid applications where value to consumers is clearly demonstrated. In fact, a 2006 FERC study found that cooperatives lead the industry in installation of smart meters, and for years have directly managed over six percent of cooperative peak load. Cyber-security, especially for systems involving higher amounts of cyber components is very important. The industry, local, state and federal governments, and the vendor community must work closely together to mitigate vulnerabilities and excess costs that can arise when government policies, industry practices and technological goals do not match.

I was also asked to address several specific points about the Committee's draft cyber-security legislation. NRECA agrees with our industry counterparts about the specifics of the legislation and supports the written testimony provided by American Public Power Association and EEI on these points.

Conclusion

In conclusion, NRECA supports the House discussion draft, with the specific language options proposed by the associations. Like our industry counterparts, NRECA is prepared to assist the Subcommittee and full Committee with advancing this legislation. NRECA also looks forward to the continued cooperation with FERC that has been a hallmark of the process of arriving at this draft. I look forward to answering any questions you may have.

Mr. BOUCHER. Thank you very much, Mr. Lawson, and we thank each of the witnesses for their testimony here today. Mr. Naumann, maybe you can answer the question about cost of implementation. Using the NERC advisory as the standard, realizing that Mr. Kelliher is suggesting that it probably didn't go far enough and that he thinks to completely address the Aurora vulnerability that steps beyond that should be taken.

But leaving that aside, just use the NERC advisory as the foundation. What would it cost a typical investor-owned utility to comply with that NERC advisory?

Mr. NAUMANN. Mr. Chairman, could I have one second to consult with Mr. Hill who probably can get me that answer?

Mr. BOUCHER. In the interest of getting the information, of course.

Mr. NAUMANN. Thank you, Mr. Chairman. Mr. Chairman, to comply with the Aurora vulnerability as we were told, and we believe we are fully compliant, was a relatively minor cost for across the entire Exelon Company, and that included the nuclear stations, which technically were not part of the advisory.

Having said that, we understand from listening to Chairman Kelliher that they believe that there are additional vulnerabilities too that were not covered by the advisory and that we don't really know about. It would be very hard to estimate the cost without knowing what the vulnerability is, nor what the recommended mitigation is and——

Mr. BOUCHER. Which is why I phrased the question only in terms of the NERC advisory.

Mr. NAUMANN. Yes, sir.

Mr. BOUCHER. Well, I am pleased by your answer that it is a relatively minor cost. Is there a dollar figure attached to that relatively minor estimate?

Mr. NAUMANN. We don't have it now. If you want, we can try to obtain that.

Mr. BOUCHER. It would be helpful. If you could just send us a letter addressed to the subcommittee following this hearing that states what you think the dollar cost to Exelon would have been across your company to meet the recommended security measures contained in the NERC advisory. That would be very helpful to us.

Let me extend that question to others on the panel who might want to respond on behalf of their associations. Ms. Kelly, Mr. Lawson, do you have any answer to what the cost per covered entity would be?

Ms. KELLY. I do not have any such answer for you at this time. We could obviously provide that for the record.

Mr. BOUCHER. It would be helpful if you could. Mr. Lawson.

Ms. KELLY. And we will look to primarily the three utilities that came in and met, from our membership, with FERC to discuss the vulnerability and what they had done. But I would like to state, and I think Mr. Lawson may be able to elaborate, that there really is a question even as to the NERC advisory as to what constituted compliance and it was not necessarily as clear as it might have been. And so, there was certain—we weren't sure what bar we were being asked to meet. And I think that was a concern.

Mr. BOUCHER. Well, I am trying to get as broad an estimate as possible. We are in the posture now of statutory drafting where we are going to be making some decisions in the very near term about how we empower FERC to move forward with its rulemaking on this subject.

Now, a key part of those considerations will be timeframes under which we expect that actions will be taken, actions taken by the FERC, yet advancing its rulemaking process to conclusion. And then actions that would be taken by the covered entities to comply with the rules that FERC puts forward. We may or may not have specifications within the statute that address the latter part of that. But having some understanding of cost and to the extent that you would want to comment on it, other kinds of implementation challenges that you might foresee would assist us in that.

Now, as Mr. Naumann pointed out, I fully realize that making definitive decisions about this are difficult at this stage because we really don't know what FERC would choose to do beyond the NERC advisory in terms of steps that would be required for covered entities. So probably our decision will be to simply empower FERC to set the timeframes for compliance by the covered entities.

It would be difficult for us to establish that statutorily, but there may be those on our panel who want to do that. So having some information about what the cost to you would be, what other implementation issues you see, just using the NERC advisory itself as a foundation would be helpful to us.

Mr. Lawson, would you have any comment about this?

Mr. LAWSON. Similar to Susan Kelly's comments in that we don't have cost info from the individual cooperatives. I think the best we could do would be to talk to the cooperatives that did meet with FERC on the Aurora advisory and see if they have that kind of information that they can provide us.

It is important to understand that cost can vary depending on the scope of the assets at each utility. It is going to be very difficult to have a typical cost. And also what I would be asking the cooperatives would be their cost associated with the language specifically in the NERC advisory.

Mr. BOUCHER. OK, that would be fine. Let me move to one other question, and again I will ask you as I have asked Mr. Kelliher to be somewhat brief in this answer. I would be interested in your views, succinctly spoken, on three questions. Number one, do you believe that the authority that we will be conferring on the FERC to guard against cybersecurity attacks should go beyond the cybersecurity and actually cover physical attacks that might be made on the covered facilities? That is number one.

Number two, address, if you will, the question of sunsets on FERC actions, FERC orders. In the first category would be the basic steps that all covered entities would have to take in order to address the Aurora vulnerability specifically. I can tell you my own view is that ought to be permanent in nature. But if you disagree with that, I would like to hear a reason why.

And the second category is steps that would have to be taken by the covered entities under FERC order pursuant to a presidentially declared unique emergency. Should there be a sunset on those or-

ders? And if so, what should be the conditions that trigger the sunset?

And then number three, what should be the basic scope of the authority that we extend to FERC with regard to the covered entities themselves? Should it just be the continental United States bulk power system? Or should it extend to Alaska and Hawaii and their separate electrical systems? And should it extend to the distribution systems in our larger cities? And I know, Ms. Kelly, you addressed that at some length in your testimony, but I would like to hear what other witnesses have to say.

So in view of the fact that Mr. Shimkus is eagerly awaiting his question time, let me ask you to be as succinct as you can in providing that answer. And who would like to begin? Mr. Sergel?

Mr. SERGEL. Address a couple of those for you. Our role here is to make sure that we can seamlessly and effectively implement whatever legislation you pass and do that and further the good work that was established when you enacted section 215 and created an ERO. So that is where I come from.

I think with respect to how broad is the authority, the highest priority is the bulk power system. That doesn't mean there aren't important things in the distribution system. There are, and let me be clear to the extent that the bill doesn't cover that, that will leave open something. That will make me uncomfortable that that is uncovered, but the higher priority is the bulk power system.

Hawaii and Alaska are special considerations, and maybe that is independent of distribution. And potentially you could look at it that way because that is even a greater concern.

With respect to the sunset provisions, we are going to be able to implement that successfully regardless of what those provisions are. With respect to the authority and how it is granted, we will seek to implement it effectively as written. But the clearer that authority is, and the better that that is laid out, certainly we will be able to implement it better.

And finally I would say with respect to—and I think the language in the draft that I looked at was "and other national security treats." Again with respect to that, clearly cybersecurity is the highest priority here. It is the simple one that is most important. It is what we have been focusing on. It is not to minimize other national security here in this context, but we understand those better. We have other ways of doing those things. It is not the highest priority for me.

Mr. BOUCHER. Thank you, Mr. Sergel. Ms. Kelly.

Ms. KELLY. Thank you. Your first question had to do with the physical attacks, and I will start there. The association position is no, that they should not be covered in this legislation and in part for the reason that Mr. Sergel just stated is that there are other governmental authorities and entities. And I would just note the FBI, the Department of Energy, state and local law enforcement that are all involved in those activities. And we already have to answer to a substantial number of masters in that regard.

Second, the sunset question you asked. The association position is that that should apply to both the interim authorities that are exercised under B, and the emergency authorities under C. Our reasoning for that was that—I am sorry?

Mr. BOUCHER. Go ahead.

Ms. KELLY. OK, our reasoning behind that was that we regarded this as stopgap emergency authority for events that would either be time limited and thus would expire by their own terms or should be replaced by NERC set reliability standards. For that reason, we wanted the sunset to apply in both cases. We negotiated with the FERC over that. They did not like the so-called hard sunset. We reached, you know, OK, well, we understand that position. And for that reason, we agreed that it could continue past the year so long as there was a determination that a problem was still existing. Our thought was in most cases that NERC reliability standards should be in place by the end of that year, and therefore it would be a moot question.

But we understand that there is a difference of opinion, and that is legitimate.

Mr. BOUCHER. Well, with regard to these interim standards that are designed to address the Aurora vulnerability, the Aurora vulnerability is not going to go away as a security threat. And steps will need to be taken therefore on an ongoing basis to address that threat. And I gather from your testimony that you are suggesting that the FERC should not be the perpetual agency to impose the requirements for what those steps ought to be.

And I gather from what you are saying that you think that the NERC, through its consensus-based rulemaking process, should take a hand off of that authority after some period of time. Have I correctly interpreted your comments?

Ms. KELLY. I think that is, yes, that is correct. Our view is that we understand the need for FERC to step in to act quickly, but we believe that that needs to then be run through the NERC standard setting process. In part, one of the reasons is, we in the industry, we think we actually have some expertise to offer on the best way to implement these standards.

And we are also concerned about cost. Let me just say that. And we want to make sure that these standards, you know, especially if they are going to be in effect for a long time, are done in the most cost effective manner possible. And that is one of the things that the industry can bring to bear. Its expertise can come to bear during the NERC standard setting process. So we are not kicking about FERC getting this authority under B to, you know, act to do this rulemaking on an expedited basis, but we are saying it should then be handed off to NERC.

Mr. BOUCHER. All right, thank you. That is very clear. Mr. Naumann?

Mr. NAUMANN. Yes, Mr. Chairman, on your first question, the draft now has the words "other national security threats." We believe that is an extremely vague term and are uncomfortable with that. You also mentioned, rather than that, physical threats. I agree with Mr. Sergel and Ms. Kelly, that is a lower priority, but if, in fact, there is going to be some additional authority beyond cyber, it should be very much tighter language than overall other national security threats, which could be interpreted as having 90-day stockpile of coal or something like that, which we think goes way beyond what——

Mr. BOUCHER. All right, that point is duly noted.

Mr. NAUMANN [continuing]. Immediate intent. And as far as the sunset, I agree with Ms. Kelly. To the extent there are interim measures for Aurora, to the extent they can be and should be replaced by permanent standards done through industry expertise, that would be our preference. And with respect to the emergency action, again I would prefer that if the requirements still remain, then the President should reissue the directive.

As far as the authority on Alaska and Hawaii, we understand that is a special situation. There are very important military installations there that somehow would need to be taken care of, but they are really not part of the schemed that we are dealing with.

Mr. BOUCHER. Major distribution systems in the cities?

Mr. NAUMANN. That is correct. Major distribution system in the city gets very complicated. We would hope that that could be done rather through consultation with the state regulatory agencies who very well understand those systems, which New York is somewhat unique. D.C. is somewhat unique. Chicago is completely different from those systems and served differently. And where do you get the cutoff on the distribution if you don't go all the way? Thank you, Mr. Chairman.

Mr. BOUCHER. All right, thank you. Mr. Lawson?

Mr. LAWSON. I agree with the comments you have heard from the other panelists. In addition, with regard to going beyond cybersecurity in the legislation, to reiterate what Mr. Naumann stated about the vagueness and broadness of the definition that we were provided, that was problematic, and we would very much want that tightened up before we could agree to anything.

Also it is very important to recognize that the industry has been dealing with physical threats for decades and has done an excellent job dealing with physical threats. Cyber threats are the new issues here. That is where the new focus should be, and that is why this legislation should focus on the cyber threats. The industry is doing a very good job with dealing with the physical threats and has for a long, long time.

With regard to the sunsets, if an order or a directive needs to continue, there are provisions in the legislation for that, for a certain period of time. However, other than the order or directive, we want the industry, through NERC's standards development process, to take care of those issues with standards. And as I mentioned in my oral statement about the expedited standards development processes that NERC does have, we think that would be an excellent vehicle for addressing some of those issues. With regard to the scope going to the distribution side of things or Alaska and Hawaii, with regard to distribution, of course, the states and local authorities have many regulatory authorities in those areas.

It is also important to realize that the bulk power system is where you can have the larger impacts. The distribution system is local, and it is broken up into many small pieces. And those impacts are often shorter in timeframe and much more limited in the numbers of meters that are not in service because of an incident.

So we think those are reasons why this legislation should focus on the bulk power system.

Mr. BOUCHER. Mr. Lawson, thank you very much. I would like to, at this time, call on the gentleman from Illinois, Mr. Shimkus, for 5 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. Mr. Naumann, please explain how your company has prepared itself for the tested and—I am sorry—and tested its response to cybersecurity threats.

Mr. NAUMANN. Thank you, Congressman. In my testimony, I referenced defense and depth, and that includes—and I guess I am going to use a number of technical words that we do. We segregate the networks that we have. We have a program of patch management, much like in a way to say you get updates on your Microsoft software occasionally when there is a vulnerability found. We do this on a very routine basis, sometimes on an emergency basis.

We have intrusion detection sensors that we maintain on our network systems. We have security event monitoring, vulnerability testing. One of the things I mentioned in my testimony is we hire outside firms to do penetration testing. In other words, they act as the red team to try to break into our system, and we then learn from what they tell us.

We deal all the time with security vendors, with the FBI, with local law enforcement. And lastly, we have encrypted our data even to the point of, for example, the laptop that I carry with me. The data is encrypted so that if it is stolen, the data is worthless to somebody.

Those are some of the measures that we take, Mr.—

Mr. SHIMKUS. This is a real pressing issue, and I know, based upon the Aurora event and others, I follow the captive nations, the former captive nations of the eastern bloc countries. Russia conducted a cyber attack against Estonia, I guess, a year and a half ago. The prelude into the intervention into Georgia was a cyber attack there. I mean so this is real stuff, and that is why it is important. And I appreciate the chairman identifying it as so.

For you again, Mr. Naumann. What resources and/or information would make your efforts to defend against cybersecurity threats more effective?

Mr. NAUMANN. Congressman, probably the most important thing is access to information. As I said, we are actively engaged in protecting our system against those threats that we know and those threats that we can try to figure out.

We understand for good security purposes, there is information that we don't have access to, and there needs to be a way that the industry can work with the government and the government can work with the industry so that we can have access to that information so that we understand what the vulnerabilities are and so that we can agree on mitigation measures to do that. Without that, we feel like we are fighting this battle with one hand tied behind our backs.

Mr. SHIMKUS. Yes, let me ask about the emergency and interim authority issues and with our border friends, the Canadians and Mexico. And what do we think their response would be? And is there some optimism? And this is for the panel as a whole, so why don't we just start from left to right. My left, your right.

Mr. SERGEL. We work very effectively with our partners in Canada and to a lesser extent with Mexico as well. NERC has a rela-

tionship with each of the eight provinces as they have decentralized responsibility for this in Canada, and those relationships are different.

I think the single most important thing to keep that relationship positive as it is today is to separate the standard setting process, which is what we do through section 215 as enabled by you in the United States, to keep that separated from the emergency measures that one would take because of an imminent threat. As long as we keep those separate, then I think we will be successful.

So we support the bill, support a bill here to take emergency action. Lots of discussion of that this morning. There needs to be a handoff of that to the standards process. If we do that, then we will work very effectively with our neighbors.

Ms. KELLY. I would just like to note that the Canadian Electricity Association submitted a statement for the record, which I would recommend for your review. I would note also that I was somewhat disturbed by Mr. Kolevar's discussion about giving FERC interim standards writing authority. That is the first that we have heard of that. It goes exactly to the issue that Mr. Sergel just identified, which is the way the 215 scheme is set up is that industry and NERC together write the standards. That is not a government activity.

So that, I think, in particular would alarm the Canadians because they have to be—they have to abide by NERC's standards. So in effect, what is happening there is they are being asked to abide by standards written by a Federal Government U.S. agency. And that is a problem, I believe. I will let them speak for themselves, but just based upon what I know during our negotiations, I think that would be a concern.

Mr. SHIMKUS. And you all can chime in if you want, but it is probably not a concern that you all would have. So what are our vulnerabilities? Is our grid adequately protected by firewalls and passwords? Will a one-time cyber reliability rule solve the problem? Or will we have to constantly change and upgrade to keep up with the changing threats? Then, this is a one over the world question. Won't government authority to constantly change protections and systems risk express an unpredictable cost on system operators?

Well, it is really for all because the question is, as we firewall and protect, bad guys evolve, which is for you. But then the question is for industry or for the rural, at what cost? How do we manage both, and we try to get it as right as we can?

Mr. SERGEL. I think standards can take you just so far because there is an opportunity to harden the system, to defend against those things which we understand like passwords and firewalls and have those be as effective as possible. We have done that with the standards in the past. They were developed cooperatively with the industry, and that process needs to evolve.

But I think it also suggests that a standard is out there to be seen. Everyone knows what we are doing, how we are proposing to implement it, and therefore, it is suggested that we have to be constantly vigilant and adapt as new problems arise.

Mr. SHIMKUS. Thank you. Ms. Kelly.

Ms. KELLY. I would just add to that that we are concerned on an ongoing basis about the cost of compliance. There is no question

about that. That was one of the reasons why our definition of cybersecurity threat is a little tighter than that that the commission supports because, for example, we would not want to be spending unknown amounts of time on new hardware, new software, new hardening, that kind of thing, for something which may not have a substantial possibility of disrupting the operation of the bulk power system.

And since theirs is phrased in the disjunctive, I believe that could possibly be the case. So I just note that for you.

Mr. SHIMKUS. OK, thank you. Mr. Naumann.

Mr. NAUMANN. Congressman, I have two things to add. The first is we are always on our own trying to protect against new threats and upgrading our equipment. And, as Mr. Sergel said, a standard can only take you so far when something new is discovered.

Mr. SHIMKUS. And plus you have the risk of great loss.

Mr. NAUMANN. We have our self-interest here.

Mr. SHIMKUS. Right.

Mr. NAUMANN. But what I would say is that that is where the consultation between the government agencies and the users, owners, and operators is useful in both working out the mitigation and dealing with the cost effectiveness as we do have experience in how to do this and we will do it. Obviously we don't want an incident, but to work together to try to design the best way to do this and protect the electric power system.

Mr. SHIMKUS. And Mr. Lawson.

Mr. LAWSON. Just to add, I think it is important to understand that utilities deal with cyber issues every day because it is important to their business, and it is important to the service they are providing to their customers. It is not something that we deal with only because we have cybersecurity standards. It is because it is the right thing to do. It is the important thing to do.

Mr. SHIMKUS. That is all I have, Mr. Chairman. Thank you.

Mr. BOUCHER. Thank you very much, Mr. Shimkus. I am going to ask unanimous consent—Mr. Shimkus and Mr. Upton have already approved this—that we insert a——

Mr. SHIMKUS. You don't want me messing with you, right?

Mr. BOUCHER. Well, yes, that was the implication of the question. These are statements from the National Association of Regulatory Utility Commissioners, the Electric Consumers Resource Counsel, and the Canadian Electricity Association, all addressing the issue before the subcommittee today, to be included in the record. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. BOUCHER. That was perfect. Thank you so much.

I want to thank our witnesses for their attendance today, for their very helpful testimony. We appreciate the time you have taken with us. We will look forward to your submission of the information that you have said you will supply to us.

And as we take further steps in this process, we will be consulting with you. With that and thanks to the witnesses, this hearing is adjourned.

[Whereupon, at 1:27 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. JOHN D. DINGELL

Today's hearing focuses on how to help ensure the reliability of our Nation's electricity grid in the face of its vulnerabilities to cybersecurity attacks.

A successful remote cyber attack on a power plant's utility control systems could do more than cause a brief black out or brown out. The Idaho National Laboratories has shown how a hacker can remotely turn a large generator into a smoldering piece of scrap metal in minutes. Known as the "Aurora" Vulnerability, this type of attack could destroy generating equipment and impair the generation and delivery of electricity across North America for weeks or months, its consequences cascading on consumers, our economy, our health care system, and our national defense assets.

These concerns are more than theoretical. A 2005 Federal Energy Regulatory Commission staff report identified 20 separate domestic and foreign instances of cyber attacks on electricity systems including hydroelectric dams and nuclear power plants. The Defense Science Board reports that U.S. grid control systems are continuously probed electronically, and "there have been numerous attempted attacks on the Supervisory Control and Data Acquisition (SCADA) systems that operate the grid."

We have been fortunate that the United States has not experienced a major power outage from a cyber attack. However, the CIA has identified cyber attacks on the electrical systems in major cities overseas which caused significant blackouts. CIA has reported that criminal enterprises have broken into utility control systems overseas as part of extortion schemes.

Since many of these same control systems used in the United States are also used in plants around the world, the knowledge about how these systems work is globalized.

In response to Department of Homeland Security's warnings about the Aurora vulnerability, the North American Electric Reliability Corporation (NERC) issued an advisory in June 2007 which outlined immediate and longer term mitigation measures for utilities. Compliance, however, was voluntary.

A FERC audit of 30 utilities found that only two or three had adequately mitigated the Aurora vulnerability and the vast majority had not complied with NERC's advisory. For some of the Nation's largest utilities, there has been woeful inaction some 15 months later.

As the Electricity Reliability Organization designated under section 215 of the Energy Policy Act of 2005, NERC is developing consensus cyber protection standards. However, this process is not responsive to the immediacy of the vulnerability or the threat. Both the Department of Energy and FERC have urged that Congress extend Federal authority to take emergency actions to protect the grid.

I commend Chairman Boucher for holding this hearing, and tackling the job of building a bipartisan consensus on legislation which will ensure that the Federal Government has the necessary powers to intervene when there are emergencies that threaten our Nation's electricity supply.

I welcome Representative Jim Langevin, Chairman of the Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, and commend him for his leadership and cooperation in working with this Committee on cyber vulnerabilities in the utility grid.

I also welcome our panel of witnesses. I hope they can inform us on whether emergency powers should extend beyond the Bulk Power System to utility systems in Alaska, Hawaii, or Guam, and to what extent these powers should also be able to reach critical distribution systems in places like the District of Columbia or New York City. We want to be sure that legislation addresses threats to the electrical system, and that the Federal Government is not improperly hobbled by legal and jurisdictional boundaries in the case of an emergency.

N A R U C
National Association of Regulatory Utility Commissioners

September 10, 2008

The Honorable Rick Boucher
Chairman
House Committee on Energy and Commerce,
Subcommittee on Energy and Air Quality
2187 Rayburn HOB
Washington, DC 20515

The Honorable Fred Upton
Ranking Member
House Committee on Energy and Commerce,
Subcommittee on Energy and Air Quality
2183 Rayburn HOB
Washington, DC 20515

Dear Chairman Boucher and Ranking Member Upton:

On behalf of the National Association of Regulatory Utility Commissioners, I respectfully request that the attached statement be included in the record for the hearing held on September 11, 2008 regarding "Protecting the Electric Grid from Cyber-Security Threats."

Thank you for your consideration.

Sincerely,

Charles D. Gray
Executive Director

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON ENERGY AND AIR QUALITY

STATEMENT ON BEHALF OF THE
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

ON

"Protecting the Electric Grid from Cyber-Security Threats"

September 11, 2008

National Association of
Regulatory Utility Commissioners
1101 Vermont Ave, N.W., Suite 200
Washington, D.C. 20005
Telephone (202) 898-2200, Facsimile (202) 898-2213
Internet Home Page http://www.naruc.org

The National Association of Regulatory Utility Commissioners (NARUC) would like to commend Chairman Boucher, Ranking Member Upton, and members of this Subcommittee for addressing the serious issue of cyber-security emergencies that threaten the safety and reliability of the bulk power electric grid. We would also like to commend the Federal Energy Regulatory Commission (FERC) and its Chairman, Joseph T. Kelliher, for their willingness to enter into discussions on this issue with NARUC and a large and diverse group of associations representing the various electric industry stakeholders. In particular, our thanks go out to Chairman Kelliher for his efforts to engage NARUC leadership on this issue very early in the legislative debate.

NARUC is a quasi-governmental, non-profit organization founded in 1889. Our membership includes the State public utility commissions serving all States and territories. NARUC's mission is to serve the public interest by improving the quality and effectiveness of public utility regulation. Our members regulate the retail rates and services of electric, gas, water, and telephone utilities. We are obligated under the laws of our respective States to ensure the establishment and maintenance of such utility services as may be required by the public convenience and necessity and to ensure that such services are provided under rates and subject to terms and conditions of service that are just, reasonable, and non-discriminatory.

Few issues are as complicated or poorly understood, while at the same time critical to our national security, as cyber threats to our nation's bulk power system. For this reason, NARUC has been examining the cyber-security issue in recent years through

our Committee on Critical Infrastructure. Over the past two years, the NARUC Committee on Critical Infrastructure has held panel discussions on the issue of cyber-security on utility systems with experts from the electric, gas, telecommunications, and water sectors as well as representatives from the national laboratories. The most recent discussions were held in July of this year at the NARUC Summer Committee Meetings where State commissioners and staff members engaged in extensive discussions with representatives of both FERC and the North American Electric Reliability Corporation (NERC). Through these discussions, some of which were for Commissioners only and closed to the public, our membership has gained insight to and an appreciation for the cyber threats to utility infrastructure. During our discussions we have learned that a "cyber attack" could consist of an individual shutting down the customer-complaint line at a small distribution utility with an email denial of service attack or a virus that shuts down its business operations. Any system that uses information communications systems is to some extent vulnerable. However, the main focus of cyber security preparedness should be the highest consequence events: those that lead to the widespread interruption of electric power to customers.

With that basic lesson in mind, NARUC strongly associates itself with the views and concerns expressed in the testimony presented by Ms. Susan Kelly on behalf of the American Public Power Association (APPA), and shares the views of the other associations listed in the APPA testimony in support of narrowly drafted legislation that focuses on vulnerabilities in the bulk-power system and on cyber-security emergencies on that system. The legislation must enhance and not disrupt section 215 of the Federal

Power Act and its mandatory reliability standards process, established by the Energy Policy Act of 2005. To that end, NARUC could support the House discussion draft, to the extent that it would include the specific language options proposed by the associations as referenced in the APPA testimony.

NARUC would like to make one additional recommendation to the Subcommittee as it deliberates on the staff draft. We believe that it would be beneficial for Congress to encourage and support FERC's efforts to continue working with its State commission colleagues in an effort to develop a seamless, coordinated strategy that would be implemented in the event of an imminent cyber threat to the nation's critical energy infrastructure.

Thank you for the opportunity to present these brief views regarding protecting the electric grid from cyber-security threats.

Statement for the Record of the
Electricity Consumers Resource Council (ELCON)
Before the House Energy and Commerce Committee
Subcommittee on Energy and Air Quality on
"Protecting the Electric Grid from Cyber-Security Threats"
September 11, 2008

The Electricity Consumers Resource Council (ELCON) appreciates the opportunity to comment on legislation to protect the electric grid from cyber-security threats. ELCON is the national association of large industrial electricity users. ELCON members are vitally interested in the issue of maintaining the reliability of the bulk power system at all times, including the possibility that the system be subject to cyber-security or other national security threats.

ELCON's members come from virtually every segment of the manufacturing community. As such, they produce not only the goods that are at the core of American life, they also produce goods that are essential to America's national security. ELCON members recognize that an adequate and reliable supply of electricity is absolutely necessary. Accordingly, to promote grid reliability, ELCON was one of the first non-utility participants in the North American Electric Reliability Council (predecessor to today's NERC) as well as an early supporter of creating a federal Electric Reliability Organization (ERO), a role now filled by North American Electric Reliability Corporation (NERC).

ELCON has been working with key industry associations to develop language providing FERC with the authority to respond to imminent cyber-security emergencies. These associations

have produced, and ELCON supports, the proposed draft legislation (herein, the "House discussion draft with the proposed industry language").

GENERAL COMMENTS

ELCON believes that the best way to address cyber-security matters is through the NERC. Congress authorized the Federal Energy Regulatory Commission (FERC) to approve a fair, open and inclusive organization to develop and enforce standards to assure the reliable operation of the North American grid. Congress added this authority to the Federal Power Act under Section 1221 of the Energy Policy Act of 2005 (EPAct05) creating a new Section 215 of the FPA. FERC certified NERC as this organization. The NERC reliability standard-setting process allows for a balance of interests that ensures access to expertise from industry across the continent for the development of standards with continental application. Section 215 of the Federal Power Act requires FERC approval of any standards before they become mandatory in the U.S.

ELCON is pleased that the House discussion draft makes clear that the NERC standard-setting process remains the appropriate vehicle for developing reliability standards, including cyber-security standards. But ELCON also recognizes that, given the nature of cyber-security emergencies and the need to respond quickly, it makes sense to treat cyber-security standards somewhat differently from operating and planning standards and to allow for quick action to respond to ever-changing threats. Such a process was suggested in a letter forwarded by NERC's President, Rick Sergel, to NERC's Board of Trustees and Stakeholders on July 7, 2008. In that letter, NERC suggests the establishment of a task force to "review and where appropriate

recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process." Importantly, this process would follow the NERC standard-setting model, thereby allowing for the development of cyber-security standards that would be approved by FERC and Canadian governmental authorities. In addition, ELCON is encouraged by NERC's proposals to elevate the profile of its Critical Infrastructure Protection Program, to increase its cyber-security expertise and to better coordinate with governmental authorities. We believe that such steps would allow NERC to better respond to cyber-security issues.

ELCON recognizes, however, that situations can arise that require actions to be taken immediately to avoid grid failures due to cyber-security emergencies. To the extent the current NERC processes are unable to respond to an emergency situation, ELCON agrees that in the U.S., FERC should be able to respond expeditiously to ensure that the grid is protected. The language in the House discussion draft with the proposed industry language would allow FERC to establish interim measures with respect to emergencies identified in the Aurora advisory. However, ELCON believes that such authority must be limited to cyber-security emergencies and must be of a limited duration.

SPECIFIC COMMENTS

- ELCON believes that the applicability of the new provisions should be limited to the "users, owners and operators" of the bulk power system. The practical application of the term "users, owners and operators of the bulk power system" has been developed by NERC in the NERC Compliance Registry Criteria (which has been filed with FERC).

Further, expanding the scope of the new cyber-security legislation to include local distribution facilities would raise serious jurisdictional and implementation issues while not increasing the protection of the grid from cyber-security threats.

- ELCON believes that the applicability of the new provisions should be limited to "cyber-security emergencies." Other governmental entities have more direct responsibilities relating to other "national security threats." Further, including such language could spark intense discussions that could delay the enactment of this legislation.
- ELCON believes that the new provisions should require the existence of both (1) a substantial likelihood of a malicious act and (2) a substantial possibility of disruption to the operation of the system for the federal government to conclude that there is a cyber-security threat that would trigger the need for emergency action.
- ELCON believes that the new provisions should contain a "sunset" provision such as that included in Subsection (d) (entitled "Discontinuance") in the House discussion draft with the proposed industry language.

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

STATEMENT FOR THE RECORD OF
THE CANADIAN ELECTRICITY ASSOCIATION
BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON ENERGY AND AIR QUALITY
HEARING ON
"PROTECTING THE ELECTRIC GRID FROM CYBER-SECURITY THREATS"

September 11, 2008

The Canadian Electricity Association (CEA), the national forum and voice of the evolving electricity business in Canada, is pleased to provide the following statement regarding U.S. legislation to protect the electric grid from cybersecurity threats. CEA's members account for the majority of Canada's installed generating capacity and high voltage transmission. In this statement, CEA provides comments on the House discussion draft. This statement also explains the importance of taking actions that are mindful of the interconnected nature of the North American transmission grid and the impact such actions could have on the reliability of the grid and on cross-border trade.

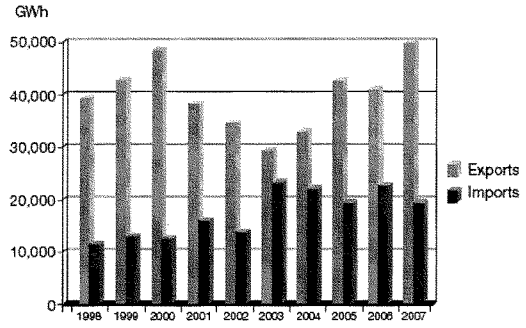
Background

The electric transmission systems of U.S. and Canadian utilities are interconnected with one another at numerous points, forming a highly integrated North American transmission grid. This integration allows for cross-border trading, which facilitates, amongst other things, a higher level of reliability for consumers, efficiencies in fuel and resource management, and efficiencies in system operation. These benefits, and the activities of companies investing and participating in markets on both sides of the border, serve citizens of the United States and Canada extremely well.

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

To provide perspective on the importance of the U.S./Canadian trading relationship, the chart below shows both exports from Canada to the U.S. and imports into Canada from the U.S. between 1998 and 2007:

Electricity Exports from Canada and Imports from the U.S., 1998-2007



Source: NEB Electricity Exports and Imports, Monthly Statistics, various years.

Canada is a net exporter of electricity to the U.S. The quantity of electricity exported from Canada to the U.S. has typically been 6 to 10 percent of Canadian production. At the same time, as the chart above demonstrates, electricity imports to Canada from the U.S. have increased over time. The North American market is borderless, and supply meets demand north to south or south to north as the market requires, to the advantage of consumers across the continent. Such electricity trade enhances the reliability of each country's electricity supply through the sale of surplus power, and mitigates risk by providing for power during times of emergency outages or periods of high electricity demand. Canadian utilities are therefore part of and therefore critical to the energy security of the United States, and the reliability of the North American transmission grid.

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

Addressing Cybersecurity Threats

The blackout of August, 2003 demonstrated the importance of carefully managing an interconnected grid for both the U.S. and Canada. In a matter of seconds, an estimated 50 million people in the Midwest and Northeast United States, and in Ontario, Canada experienced an electric power blackout. While the 2003 blackout was caused, in part, by a failure of a utility to comply with operating standards, the grid could be equally compromised following an exploitation of a cybersecurity vulnerability. CEA members are therefore sensitive to the potential for disruptions in electric service due to a system event anywhere on the international grid, including threats to cybersecurity.

CEA believes that any actions to address cybersecurity issues must be accomplished in a manner that recognizes the mutual inter-dependency of the interconnected Canada-U.S. transmission systems, and does not unintentionally imperil or downgrade reliability and erect barriers to cross-border trade. CEA believes that the best venue to address cybersecurity matters is the North American Electric Reliability Corporation ("NERC"). Through the reliability standard-setting model included in section 215 of the Federal Power Act, the NERC reliability standard-setting process allows for a balance of interests that ensures access to expertise from industry across the continent for the development of standards with continental application that can be approved by authorities on both sides of the border – be it FERC in the U.S., or any of the jurisdictional authorities in the Canadian provinces. This model recognizes jurisdictional sovereignty through the existence of remand provisions in the various pieces of Canadian and U.S. legislation underpinning the model and which is incorporated into the existing NERC standard setting procedures. This component assures that no governmental authority has the ability to unilaterally modify standards that would apply to the whole system, and that any

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

variances are accommodated through the collective process. At the same time, it gives public authorities the confidence that the system has a government backstop, providing governmental authorities on both sides of the border with the confidence that standards developed through that process reflect their concerns.

CEA does recognize, however, that situations can arise that require emergency actions to be taken immediately to protect the reliability of the bulk power system. To the extent the NERC processes are unable to respond to such an emergency situation, CEA agrees that governmental bodies should be able to respond expeditiously to ensure that the grid is protected. In terms of U.S. governmental authority to respond to imminent cybersecurity threats, CEA has been working with key industry associations to provide input to legislative language that would provide FERC with authority to respond. The language would further allow FERC to establish interim measures with respect to threats identified in the Aurora advisory. CEA understands the need for authority to address emergency situations, although we believe that such authority must be limited only to cybersecurity emergencies and must be of a limited duration. The House discussion draft incorporates the limited authority suggested by the industry associations for FERC to respond to identified cybersecurity emergencies, and CEA supports the House discussion draft with the specific language options proposed by the associations.

CEA strongly supports the inclusion in the House discussion draft of a requirement that FERC consult with appropriate Canadian authorities before taking measures to address cybersecurity threats. Unlike the U.S. system, transmission is regulated in Canada primarily by provincial governmental authorities. Moreover, reliability standards are authorized and enforced by provincial governmental authorities. Consulting with the appropriate governmental authorities in the relevant provinces will help to ensure that actions taken by FERC are respectful of Canadian jurisdictional sovereignty and avoid unintended impacts on reliability and cross-

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

border trade.[1] The absence of consultation between and among governmental authorities could further result in the elimination of, or reduction in, the sharing of critical cybersecurity information -- not a good result at a time when the sharing of information is becoming more and more important.[2]

CEA is also pleased that the House discussion draft makes clear that the NERC standard-setting process remains the appropriate vehicle for developing reliability standards, including cybersecurity standards. But CEA also recognizes that, given the nature of cybersecurity threats and the need to respond quickly, it may make sense to treat cybersecurity standards differently from operating and planning standards and to allow cybersecurity standards to be developed in a less public manner and in a way that allows for quick action to respond to ever-changing threats. In other words, NERC could establish an alternative standard setting process that would allow it to be more nimble in addressing cybersecurity issues. Such a process was suggested in a letter forwarded by NERC to NERC's Board of Trustees and Stakeholders on July 7, 2008. In that letter, NERC suggests the establishment of a task force to review "and where appropriate recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process." We would support NERC's efforts to establish a separate process for addressing cybersecurity issues. Importantly, this process would follow the NERC standard-setting model, thereby allowing for the development of cybersecurity standards that are respectful of Canadian jurisdictional sovereignty and allowing for the development of standards that can be approved by Canadian governmental authorities. In addition, CEA is encouraged by NERC's proposals to elevate the profile of its Critical Infrastructure Protection Program, to increase its

[1] The House discussion draft contains a requirement that consultation be subject to adequate protections to protect against disclosure, but FERC and the associations disagree over whether to use the term "inappropriate disclosure" or "public disclosure." For the sake of clarity and precision, CEA supports the use of the term "public disclosure."

[2] CEA also believes strongly that orders or measures to address known or imminent cyber-security threats must be accompanied by sufficient information sharing regarding the threat such that those implementing the order or measure can do so effectively.

Canadian Electricity Association
Association canadienne de l'électricité
www.canelect.ca

cybersecurity expertise and to better coordinate with governmental authorities. We believe that such steps would allow NERC to better respond to cybersecurity issues.

CEA appreciates this opportunity to provide this statement and would be happy to answer any questions that may arise during the hearing.

CEA 350 Sparks Street, suite 907, Ottawa, Ontario Canada K1R 7S8
Tel.: (613) 230-9263 - fax: (613) 230-9326 - info@canelect.ca
The voice of Canadian Electricity

350 rue Sparks, bureau 907, Ottawa, Ontario Canada K1R 7S8
Tél.: (613) 230-9263 - Téléc.: (613) 230-9326 - info@canelect.ca ACE
La voix de l'électricité canadienne

Item #	Description	Designation	Date
Index of Non-Public Hearing Documents for "Protecting the Grid from Cyber Security Threats"			
(Filed in Committee Archives)			
1	NERC Aurora Advisory	For Official Use Only	June 21, 2007
2	The Status of Aurora Mitigation on the Bulk-Power System	Internal Draft by FERC	September 8, 2008
3	Federal Energy Regulatory Commission Staff Report on Electric Supervisory Control and Data Acquisition Systems Cyber Vulnerability Assessment	Critical Energy Infrastructure Information	June 2005

The above documents are available in the archived hearing record but are not printed in the GPO version of this hearing due to their designation.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

October 24, 2008

The Honorable John D. Dingell
Chairman
House Energy and Commerce Committee
Washington, D.C. 20515-6115

Dear Mr. Chairman:

Please find enclosed my responses to your questions for the record of the Committee's Energy and Air Quality Subcommittee's September 11, 2008 hearing entitled "Protecting the Electric Grid from Cyber Security Threats." I appreciate having this opportunity to address your concerns and those of Representative Markey.

If you need additional information, I hope you will not hesitate to get back in touch with me.

Sincerely,

Joseph T. Kelliher
Chairman

Enclosure

cc: Representative Joe Barton
Representative Edward J. Markey
Representative Rick Boucher
Representative Fred Upton

The Honorable John D. Dingell

1. When the Federal Energy Regulatory Commission (FERC) audited 30 utilities for compliance with the North American Electric Reliability Corporation (NERC) Advisory regarding the Aurora vulnerability, did FERC's audit find that the Bulk Power System is not protected from the Aurora and similar vulnerabilities?

Response: FERC staff found a variety of actions taken in response to the Aurora advisory. While almost all of the entities took steps to increase their cyber security and did make it more difficult for an adversary to conduct a cyber attack, Commission staff found that most of the interviewed entities were not fully protected from the Aurora and similar vulnerabilities. This was due to a number of factors, including differences in interpretations of both the seriousness of the Aurora vulnerability and how the advisory should be implemented, in the depth of understanding about the vulnerability, and in facilities owned by the interviewed entities.

2. Did your audit find that there were utilities that had complied with the NERC Advisory, but still had Aurora vulnerabilities? Why wasn't utility compliance with the NERC Advisory sufficient to ensure that the utilities had mitigated the vulnerability?

Response: FERC staff is aware of cyber vulnerabilities that are related to the Aurora vulnerability and remote access, but were not the subject of the Aurora advisory. Thus, utilities could be considered in compliance with the advisory but still remain vulnerable to remote access attacks. In addition, we found many different interpretations and levels of understanding about exactly what companies were being asked to protect against. For the most part, FERC staff did not find utilities that had complied with the Aurora advisory but still had Aurora vulnerabilities. Rather, the problem seemed to be that entities believed that they had complied with the advisory, when in fact they had not for various reasons. As mentioned in response to question one above, there were a number of different interpretations that the interviewed entities had about what the advisory required and a variety of levels of understanding regarding the technical details of the vulnerability.

3. NERC was designated as the Electricity Reliability Organization under the Energy Policy Act of 2005. Why aren't their authorities sufficient to ensure that utilities address cyber vulnerabilities such as Aurora?

Response: Under the Energy Policy Act of 2005 (EPAct), the Electric Reliability Organization (ERO) has the authority to develop Reliability Standards and to enforce them once they have been approved by FERC. The development of such standards is to "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests..." Federal Power Act section 215(c)(2)(D). This is a time-consuming, public, and deliberative process. In contrast, the ERO's advisory process is much quicker and is primarily a one-way dissemination of information. As discussed below, the ERO's advisory process has improved since the Aurora advisory, and continues to evolve. However, the fundamental characteristic of the advisory process is voluntary compliance; no entity is required to comply and follow-up enforcement action is not authorized.

4. Is the Aurora vulnerability the only foreseeable area of concern that could fall under emergency powers?

Response: No. There are other cyber concerns, as well as physical security concerns. Also, there may be concerns that come to our attention over time. The field of cyber security is changing rapidly. Not only are new vulnerabilities being found on existing infrastructure applications, but new products and applications are becoming available that present new vulnerabilities that must be addressed. In addition, vulnerabilities or threats may be discovered that only affect a particular region or city. In such a case, the appropriate action may be very focused and not apply to the entire electric industry.

5. Did the utility industry follow your recommendations on how and where to improve their mitigation plans?

Response: We only have limited information on whether the interviewed entities took additional steps to improve their mitigation plans after the interviews. We have had follow-up conversations with some of those entities, who either have taken additional steps or are considering such steps, and have more conversations planned to discuss the actions they have taken in response to our recommendations. In addition, our review was limited to 30 industry volunteers. We do not have any additional data on how the rest of the industry has developed and implemented mitigation plans in reaction to the initial advisory from NERC.

6. How are you protecting from disclosure the information that you received during this audit on existing vulnerabilities and mitigation efforts?

Response: We intentionally received no written material regarding cyber security during the interviews to avoid concerns about our ability to protect that information from public disclosure.

7. What would be your estimate of the costs to utilities in order for them to comply with the Aurora mitigation requirements?

Response: FERC has no estimates of the Aurora mitigation costs. There would likely be a wide range of costs depending on many things, including the number and type of assets to be protected and the security measures already in place.

8. "Smart Grid" technology needs to be part of the future electric grid. You recommend that cyber security mechanisms be incorporated prior to the implementation of advanced grid architecture. Would development of cyber controls slow down or otherwise hinder future development of smart grid technology?

Response: The incorporation of cyber security mechanisms into an advanced grid architecture is one of many steps involved in implementation of smart grid technology. If cyber security is incorporated into smart grid technology while it is being developed and implemented, FERC staff does not expect that it would hinder the development of the smart grid. If, however, security is not considered during the design of smart grid technology, but, instead, considered and added after the implementation of the technology, this would likely require additional time and possible expense to achieve an adequate level of cyber protection.

9. The NERC Critical Infrastructure Protection Standards exclude nuclear plants regulated by the Nuclear Regulatory Commission. I understand that there were cyber incidents involving the Browns Ferry and Hatch nuclear power plants. Were there gaps in coverage on cyber protections? If so, please describe the gaps and suggest a resolution.

Response: Commission staff does not have information on incidents at the two plants cited. However, there are two regulatory efforts currently underway to improve the cyber security of nuclear power stations and eliminate the gaps mentioned in the question. The Nuclear Regulatory Commission (NRC) has a rulemaking underway to establish new cyber security standards that would apply to the facilities under its jurisdiction within a nuclear power station. In addition, on September 18, 2008, FERC issued an Order on Proposed Clarification (which is attached) to address a potential regulatory gap within nuclear power stations.

Under FERC's proposed clarification, the Critical Infrastructure Protection Reliability Standards, as developed by the ERO and approved by FERC, would apply to any equipment within a nuclear power station that is not regulated by the NRC. As the Commission explained in that Order, it is our understanding that the NRC regulates only the equipment within a nuclear power station that is directly associated with reactor safety, security and emergency response. Other facilities within a nuclear power station may be operated to assure continuity of electricity production and would, under our proposal, be subject to the FERC-approved Critical Infrastructure Protection Reliability Standards.

10. How would FERC enforce its cyber security measures?

Response: The mechanism for compliance monitoring and enforcement of cyber security measures would depend on the final form of the legislation enacted. Assuming the Commission is the entity that will have the authority to order measures or actions by utilities to address cybersecurity or other national security threats to the electric grid, the Commission would enforce those measures or actions. To do so, it would either utilize a process similar to the one in place now to enforce the Reliability Standards under section 215 of EPAct where the ERO has the primary responsibility to monitor and enforce the standards, or it would rely more directly on the Commission's resources for the front line monitoring and enforcement activities. Under this second approach, FERC would enforce its cybersecurity measures much as it does the remainder of the statutes, regulations and orders that it enforces. First, the Commission has extensive experience in auditing the entities it regulates on both a regular and random basis. The industry is aware of the possibility that an entity could be notified of one at any time and therefore the audit program is a strong disincentive to noncompliance. In working with the companies during an audit, the Commission identifies areas of noncompliance and assists companies in developing mechanisms to bring them into compliance. Second, the Commission staffs a hotline for enforcement-related calls and a help desk for compliance-related questions. These allow companies to seek guidance on compliance issues, and the hotline allows other entities to notify the Commission if they observe instances of noncompliance. Finally, the Commission employs a staff of lawyers and engineers to conduct investigations into instances of noncompliance. If such an investigation leads the Commission to conclude that a violation may have occurred, it is authorized to commence an adjudication to determine whether a violation occurred and, if so, what the consequences of that violation should be. Under Federal Power Act section 316A, the Commission is authorized to assess a civil penalty up to $1,000,000 per day per violation and to order remediation of the violation. If the Commission is not the entity that is given the authority to order measures or actions by utilities to

address the threats to the grid, the Commission would not have the authority to enforce those measures or actions.

11. Mr. Kolevar's testimony urges Congress to authorize DOE to use its emergency powers under Section 202[c] of the Federal Power Act to direct cyber protective actions by utilities while FERC is developing an interim cyber standard. Is FERC in agreement with this construct?

Response: Our recommendation is that Congress authorize the President, either directly or indirectly through DOE, to make the determination as to whether there is a threat, but that FERC have the authority to order measures or actions by utilities to address cybersecurity or other national security threats to the electric grid. This approach recognizes that the executive branch should determine when an imminent cybersecurity or other national security threat exists, but that FERC, in light of its expertise and existing responsibilities under the FPA to oversee the reliability of the bulk power system, should be the governmental entity that determines which measures or actions are necessary to protect the grid in response to that threat. FERC would have the ability and expertise to ensure that the appropriate measures or actions are ordered and to ensure that they are not in conflict with existing Reliability Standards.

12. The Canadian Electricity Association has submitted a written statement on this hearing's topic to the Subcommittee (attached). As you know, Canada is a net exporter of electricity to the United States and the grid is interconnected.

a. Have you discussed cyber security vulnerabilities to the Bulk Power System with federal and provincial governmental officials in Canada?

Response: The Commission has discussed cyber security and the Aurora vulnerability in general with officials of both the federal and some provincial governments. Most of these discussions were part of regularly scheduled reliability meetings designed to foster cooperation on, and exchange of, reliability-related matters and information.

b. If the answer is yes, is there a mechanism by which the Canadian governmental units and regulators would agree to mitigate cyber vulnerabilities in the event of an emergency that could also affect the reliability of the U.S. grid? If so, what is the mechanism?

Response: The Commission is not aware of such a mechanism.

c. Is additional consultation between the governments necessary to develop a joint response to a cyber emergency that impacts the grid?

Response: Additional work is needed in this area, including among the federal and provincial governments in Canada. The Commission intends to continue its efforts to improve coordination with the Canadian governmental units and regulators.

13. Please provide examples of information which FERC would want treated as "controlled unclassified information" which could not be made public due to the risk of malicious use.

Response: In general, the designation could be used to protect information regarding a security vulnerability or threat, the proposed mitigation measures to address the vulnerability or threat, and the timeline and mitigation measures employed by the affected entities. Examples could include information about specific equipment or software utilized by an entity or entities, security steps taken by an entity or entities, or information about successful or attempted cyber incidents. It is important to note, however, that treating information as "controlled unclassified information" under current law does not protect this information from public disclosure under the Freedom of Information Act.

14. Has the FERC fully implemented all of the recommendations and eliminated all of the vulnerabilities identified in the Inspector General's report entitled The Federal Energy Regulatory Commission's Unclassified Cyber Security program, 2008 (DOE/IG-0802)?

Response: The Commission is on track to complete the thirteen actions necessary to fully remediate the security vulnerabilities and implement the recommendations identified by the Inspector General's report (DOE/IG-0802) within the timelines agreed to by the Commission and the Inspector General. All actions will be completed by December 31, 2008.

The Honorable Edward J. Markey

1. It is clear from the testimony from all of our panel participants that the cybersecurity threat is serious. Could you tell me, on a scale of 1 to 10, with 10 being the most vulnerable, how you would rate the grid's vulnerability to the threat of a cyber security incident?

Response: The grid's vulnerability to cyber security threats differs from location to location. In general, Commission staff estimates that the grid's vulnerability is rated within the upper half of the scale. However, staff also believes that when the new Critical Infrastructure Protection Reliability Standards are implemented in 2010 and coupled with a diligent compliance monitoring and enforcement program, improvements in grid security will occur.

2. Your testimony also states that "much work remains to be done and, in large part, the Aurora threat remains." You also explain that the standards developed by NERC were insufficient, and FERC ultimately stepped in to do an expansive amount of work on the Aurora vulnerability. Given the high degree of vulnerability of our grid system and this clearly deficient response from the industry, what grade would you give NERC in its handling of this vulnerability and what grade would you give FERC?

Response: NERC's Aurora advisory was the first such advisory issued by the ERO after the passage of EPAct. NERC recognizes that the communication of the advisory and the mitigation measures necessary to address the Aurora threat were not sufficient. Accordingly, NERC has taken steps with subsequent advisories to ensure that relevant entities receive timely and adequate communication of the information in an advisory. FERC will also work with NERC to improve the content of the NERC advisories and better understand industry's compliance with them. For instance, NERC issued the Aurora advisory on June 15, 2007 and in turn, FERC issued an order on September 20, 2007 requiring that all subsequent advisories be submitted to Commission staff for review as soon as possible before they are issued. In addition, FERC ordered that a summary of the affected entities' compliance with the advisory should be sent to the Commission no later than 30 days after the applicable deadline in the advisory. But it is important to recognize the limits of a voluntary advisory process. Under current law there is no authority to require users, owners and operators of the grid to take any action except in the context of an approved reliability standard. Thus, it is not reasonable to expect complete mitigation of a cybersecurity problem such as Aurora through this process. Given the limitations of the existing authority, NERC acted reasonably to craft and issue an advisory in conjunction with DHS and DOE. FERC likewise acted responsibly to collect information regarding responsiveness to the advisory, interviewing a sample of volunteers in order to obtain relevant information about mitigation efforts in a timely manner. But without authority to order mandatory action to mitigate the Aurora threat, neither entity can achieve timely mitigation of this vulnerability.

2. I believe the response to the Aurora vulnerability has been unacceptably slow and inefficient. But looking forward, rather than back, please tell me when you believe you will be able to report that the Aurora vulnerability is no longer a threat to our grid? Please provide a detailed timeline as to what must occur to make this happen?

Response: Currently, many utilities are tying their Aurora mitigation efforts to their efforts to comply with the Critical Infrastructure Protection (CIP) Reliability Standards. The implementation plan for those standards generally requires transmission owners and generation owners to be compliant with the requirements of the standards before 2010. Other entities, such as balancing authorities and transmission operators, are generally required to comply by July 1, 2009. However, there are major questions regarding the implementation of the Reliability Standards and the resulting effectiveness of Aurora mitigation efforts. The CIP standards require protection of critical assets and critical cyber assets, not all assets. Similarly, most entities interviewed by Commission staff are only planning Aurora mitigation measures for critical assets. The CIP standards currently allow for individual discretion as to the identification of which assets are affected by the standards. In addition, FERC identified terms such as "reasonable business judgment," "acceptance of risk," and exemptions for technical feasibility issues that can provide discretion as to the application and subsequent effectiveness of the CIP standards. Under its authority, FERC ordered the removal or restriction of these terms in the standards; however, under section 215 of the FPA the Commission cannot make these changes directly but can only order the ERO to develop them through a stakeholder process. As a result, questions such as whether the Aurora mitigation measures will be consistently applied to the appropriate assets, how well entities understand the details of the Aurora vulnerability and the effectiveness of their mitigation steps, and how effectively the standards will compel mitigation remain. These questions will require follow-up efforts to evaluate. Of course, under current law, mitigation steps that go beyond those required to comply with the Reliability Standards will be voluntary. Thus, we cannot reasonably predict when we will be able to report that the Aurora vulnerability is no longer a threat. It is also important to note that FERC staff is aware of cyber vulnerabilities that are related to the Aurora vulnerability but are different remote access vulnerabilities. These vulnerabilities were not the subject of the Aurora advisory.

3. In a report released in November 2003 regarding the Northeast Blackout, the General Accounting Office identified some actions FERC should take to better ensure the security of the nation's grid. One recommendation provided by GAO, and a particularly timely one given the increased interest in energy production, was that FERC should better integrate sufficient security measures for critical

systems into the planning for new construction or the upgrading of existing infrastructure, rather than viewing them as later add-ons. Has FERC implemented this suggestion, and if so, how? If not, why not, and when does FERC predict it will have progress to report on this front?

Response: We assume this question relates to the general recommendation in the report regarding the integration of security measures into planning for new construction. Under section 215 of the FPA, FERC's method of assuring adequate security measures for critical systems, both new and existing, is through mandatory reliability standards. The Commission currently does not possess authority to direct or condition construction of new infrastructure on the electric grid, with limited exceptions. Thus, its only method of assessing the adequacy of security measures for both new and existing systems is compliance with Reliability Standards approved under section 215 of the FPA. Without additional authority to take immediate, enforceable action, the Commission's ability to achieve this recommendation is limited.

124 FERC ¶ 61,247
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM06-22-000]

Mandatory Reliability Standards for Critical Infrastructure Protection

(Issued September 18, 2008)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Order on Proposed Clarification.

SUMMARY: The Commission is proposing to clarify that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706.

DATES: Comments are due **30 days from the date of issuance of the Commission order.**

ADDRESSES: You may submit comments, identified by docket number by any of the following methods:

- Agency Web Site: http://ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Commenters unable to file comments electronically must mail or hand deliver an original and 14 copies of their comments to: Federal

Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, D.C. 20426.

FOR FURTHER INFORMATION CONTACT:

Jonathan First (Legal Information)
Office of General Counsel
888 First Street, NE
Washington, D.C. 20426
(202) 502-8529

Regis Binder (Technical Information)
Office of Electric Reliability
888 First Street, NE
Washington, D.C. 20426
(202) 502-6460

SUPPLEMENTARY INFORMATION:

124 FERC ¶ 61,247
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Joseph T. Kelliher, Chairman;
Suedeen G. Kelly, Marc Spitzer,
Philip D. Moeller, and Jon Wellinghoff.

Mandatory Reliability Standards for Critical Infrastructure Protection — Docket No. RM06-22-000

ORDER ON PROPOSED CLARIFICATION

(Issued September 18, 2008)

1. In this order, the Commission proposes to clarify the scope of the eight Critical Infrastructure Protection (CIP) Reliability Standards[1] approved in Order No. 706 to assure that no "gap" occurs in the applicability of these Standards.[2] In particular, each of the eight CIP Reliability Standards provides that facilities regulated by the U.S. Nuclear Regulatory Commission (NRC) are exempt from the Standard. It has come to the attention of the Commission that the NRC does not regulate all facilities within a nuclear generation plant. Thus, to assure that there is no "gap" in the regulatory process, the Commission proposes to clarify that the facilities within a nuclear generation plant in the

[1] Reliability Standards CIP-002-1 through CIP-009-1. Reliability Standard CIP-001-1, which pertains to sabotage reporting, does not include the exemption statement that is the subject of this order.

[2] Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, order on reh'g, 123 FERC ¶ 61,174 (2008).

United States that are not regulated by the NRC are subject to compliance with the eight CIP Reliability Standards approved in Order No. 706.

2. Comments on the Commission's proposed clarification are due 30 days from the date of issuance of this order, after which the Commission intends to issue a further order on the matter.

Background

3. The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), developed eight CIP Reliability Standards that require certain users, owners and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. In January 2008, pursuant to section 215 of the Federal Power Act (FPA),[3] the Commission approved the eight CIP Reliability Standards. In addition, pursuant to section 215(d)(5) of the FPA,[4] the Commission directed the ERO to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission.

4. Each of the eight CIP Reliability Standards includes an exemption for facilities regulated by the NRC. For example, Reliability Standard CIP-002-1 provides:

---

[3] 16 U.S.C. § 824o (2006).

[4] 16 U.S.C. § 824o(d)(5).

> The following are exempt from Standard CIP-002: Facilities Regulated by the U.S. Nuclear Regulatory Commission . . . . [5]

5. In an April 8, 2008 public joint meeting of the Commission and the NRC, staff of both Commissions discussed cyber security at nuclear generation plants. While NRC staff indicated that the NRC has proposed regulations to address cybersecurity at nuclear generation plants,[6] NRC staff raised a concern regarding a potential gap in regulatory coverage. In particular, NRC staff indicated that the NRC's proposed regulations on cybersecurity would not apply to all systems within a nuclear generation plant. NRC staff explained:

> The NRC's cyber requirements are not going to extend to power continuity systems. They do not extend directly to what is not directly associated with reactor safety security or emergency response. . . .
>
> As a result, and when you look at the CIP standards that were issued, there is a discrete statement in each of the seven or eight standards where it specifically exempts facilities regulated by the United States Nuclear Regulatory Commission from compliance with those CIP Standards. So

---

[5] Reliability Standard CIP-002-1, section 4.2 (Applicability).

[6] Nuclear Regulatory Commission, Notice of Proposed Rulemaking, Power Reactor Security Requirements, NRC Docket No. RIN 3150-AG63 (Oct. 2006).

there is an issue there in the sense that our regulations for cyber security go up to a certain point, and end.[7]

Discussion

6. The Commission shares the concern raised at the April 8, 2008 joint meeting. It appears that the NRC's regulation of a nuclear generation plant is limited to the facilities that are associated with reactor safety or emergency response.[8] The Commission believes that a nuclear generation plant will likely include critical assets and critical cyber assets that are not safety related and, therefore, not regulated by the NRC. For example, facilities that pertain to the "continuity of operation" of a nuclear generation plant may be necessary for the generation of electricity that affects the reliability of Bulk-Power System, but not have a role in reactor safety. The Commission understands that such facilities would not be subject to compliance with cyber security regulations developed by the NRC.

7. The Commission believes that the plain meaning of the exemption language in the eight CIP Reliability Standards at issue is that only those facilities within a nuclear generation plant that are regulated by the NRC are exempt from those Standards. The exemption language in the eight CIP Reliability Standards neither states, nor implies, that

---

[7] April 8, 2008, Joint Meeting of the Nuclear Regulatory Commission and Federal Regulatory Commission, Tr. at 77-78.

[8] See id. See also 42 U.S.C. §§ 2133, 2201 and 2232.

all facilities within a nuclear generation plant are exempt from the Standards, regardless of whether they are subject to NRC regulation. However, the Commission believes there is a need to assure that there is no potential gap in the regulation of critical cyber assets at nuclear generation plants and to assure that there is no misunderstanding of the scope of the exemption in the CIP Reliability Standards. The Commission, therefore, proposes to clarify that Reliability Standards CIP-002-1 through CIP-009-1 apply to the facilities within a nuclear generation plant that are not regulated by the NRC.

8. To be clear, the Commission's intent is to eliminate a potential gap in the regulation of critical assets and critical cyber assets at nuclear generation plants in the United States. The Commission reaffirms the language of the CIP Reliability Standards - and respects the jurisdiction of the NRC – and does not intend that those Standards apply to facilities within a nuclear generation plant that are regulated by the NRC. This should allay concerns that a specific facility is subject to "dual" regulation by both the Commission and NRC as to cyber security.

9. In addition to comments on the proposed clarification, the Commission seeks comment on the following two related matters:

> Whether there is a clear delineation between those facilities within a nuclear generation plant that pertain to reactor safety security or emergency response and the non-safety portion or, as NRC refers to it, the "balance of plant." For example, the generator itself in a nuclear generation plant would seem to be under the CIP

Reliability Standards, but the motors that operate nuclear reactor control rods would seem to be under NRC regulation. If the delineation is not clear, is there a need for owners and/or operators of nuclear generation plants to identify the specific facilities that pertain to reactor safety security or emergency response and subject to NRC regulation, and the balance of plant that is subject to the eight CIP Reliability Standards?

In Order No. 706, the Commission approved NERC's "(Revised) Implementation Plan for Cyber Security Standards CIP-001-1 through CIP-009-1" for the eight cybersecurity Reliability Standards. The implementation plan provides a staggered approach to implementation that includes three tables with separate timelines for various industry segments. Table 3, which applies to generation owners and generation operators, requires achieving compliance with the requirements of the CIP Reliability Standards by December 31, 2009. The only requirement that has a different compliance date in Table 3 is CIP-003-1 Requirement R2, which must be complied with by June 30, 2008. The Commission seeks comment whether Table 3 for generation owners and generation operators should control the implementation schedule of the CIP Reliability Standards to the facilities within a nuclear generation plant that the NRC does not regulate.

10. Comments on the Commission's proposed clarification are due 30 days from the date of issuance of this order, after which the Commission intends to issue a further order on the matter.

The Commission orders:

The Commission directs that this order be published in the Federal Register. Comments on the Commission's proposed clarification are due 30 days from the date of issuance of this order.

By the Commission.

(SEAL)

Kimberly D. Bose,
Secretary.

Department of Energy
Washington, DC 20585

December 16, 2008

The Honorable John D. Dingell
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On September 11, 2008, Kevin M. Kolevar, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, testified regarding, "Protecting the Electric Grid from Cyber Security Threats."

Enclosed are the answers to eight questions that were submitted by you to complete the hearing record.

If we can be of further assistance, please have your staff contact our Congressional Hearing Coordinator, Lillian Owen, at (202) 586-2031.

Sincerely,

Lisa E. Epifani
Assistant Secretary
Congressional and Intergovernmental
Affairs

Enclosures

Printed with soy ink on recycled paper

QUESTION FROM CHAIRMAN DINGELL

Q1. Your testimony urges Congress to authorize the Department of Energy (DOE) to expand its emergency powers under Section 202[c] of the Federal Power Act to direct cyber protective actions by utilities while the Federal Energy Regulatory Commission (FERC) is developing an interim cyber standard. Is this a DOE position or an Administration position?

A1. The Administration has determined that DOE, with its authority under the Federal Power Act, has the requisite technical and management capabilities to implement emergency actions when necessary to protect the electric power grid from cyber attacks. The recommendations put forth in the September 11, 2008 testimony represent the Administration's position. To the extent that Congress acts in this area, the Administration recommends that it consider the following:

Allow the FERC to establish interim measures for the purpose of rapidly responding to specific electric sector vulnerabilities. These measures should include a minimum comment period.

With respect to an imminent threat the bulk power system, authorize the Department of Energy to issue an order for immediate remedial action. That order could stand until new FERC interim measures are developed. This structure could provide an effective bridge until cyber security reliability standards are developed, approved and implemented pursuant to section 215.

QUESTION FROM CHAIRMAN DINGELL

Q2. If a Presidential emergency declaration is considered, which officials, in your view, should be involved with making the decision? What are the steps that would be taken to invoke an emergency?

A2. The Administration is continuing to examine what additional authorities, if any, are appropriate for DOE and FERC. The Department recognizes that two separate actions are required to address 1) high-risk/impact vulnerabilities, and 2) imminent threats to the energy infrastructure (emergencies). High-risk/impact vulnerabilities could be addressed through an interim order or measure by FERC, with a minimum comment period, until appropriate standards are developed. An emergency would be invoked if and when credible information was presented by one of the National Intelligence Agencies that an entity may exploit a specific cyber vulnerability endangering the security and reliability our critical energy infrastructure. Intelligence information along with cyber vulnerability information would be reviewed by a cleared expert team (intelligence, energy and cyber expertise) and a decision memorandum would be presented to the Secretary regarding an emergency order. The Federal Power Act 202(c) authority was transferred to DOE by the DOE Organization Act (P.L. 95-91) and currently does not include cyber emergencies.

QUESTION FROM CHAIRMAN DINGELL

Q3. Is the North American Electric Reliability Corporation adequately equipped to deal with cyber security threats to the bulk power system? Given its consensus-based process of adopting standards, can it respond promptly enough to cyber threats identified by intelligence agencies or DOE?

A3. In accordance with the requirements set forth in the Energy Policy Act of 2005, FERC selected NERC as the Energy Reliability Organization and thereby certified that NERC had the ability to develop and enforce reliability standards, including cyber security. The adoption of cyber security standards is a critical but often time-consuming process. For example, NERC's cyber security standards have been under development since 2003 and were approved by FERC (subject to modifications) in 2008. They will not be fully implemented until December 31, 2010 (auditable). Thus, NERC is not currently equipped to respond quickly or confidentially to an imminent threat to the bulk power system.

QUESTION FROM CHAIRMAN DINGELL

Q4. Are there cyber security threats to other energy infrastructure—such as natural gas compressor stations, hydroelectric power stations, Liquid Natural Gas facilities, refineries and pipelines? If so, please describe such threats.

A4. Many of the process control systems (PCS) that are used widely across the oil, natural gas and electric sector are moving toward commercial-off-the-shelf (COTS) hardware and software. This practice makes many facilities potentially susceptible to an exploitation of a common vulnerability. The Intelligence Community (IC) has determined that our Nation's information infrastructure, including embedded processors and controllers in critical infrastructures, is being targeted by a growing array of state and non-state adversaries including hostile governments, terrorist groups, industrial spies, disgruntled employees, and malicious intruders. Cyber exploitations continue to grow and become more sophisticated and targeted. Because of the complexity and interdependencies of control systems, the need for legislation addressing sector-specific vulnerabilities must be carefully considered to minimize unintended impacts on other infrastructures.

QUESTION FROM CHAIRMAN DINGELL

Q5. Are there standards for protecting oil and gas critical infrastructure? Have these been adopted by the oil and gas industry? Is compliance with such standards mandatory or voluntary?

A5. The oil and gas sector has developed several voluntary standards that address cyber security for control systems including:

1. API Standard 1164, "Pipeline SCADA Security". API 1164 provides guidance to the operators of oil and natural gas pipeline systems for managing SCADA system integrity and security. This is specifically designed to provide the operators with a description of industry practices in SCADA security and to provide the framework needed to develop sound security practices within the operator's individual companies. API 1164 addresses access control, communication security (including encryption), information distribution classification, physical issues (including disaster recovery and business continuity plans), operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, and field devices configuration and local access.

2. AGA 12, Part 1, Cryptographic Protection of SCADA Communications. AGA 12. Part 1 focuses on the background needed to understand the threats to SCADA communications, an approach to developing comprehensive security policies that include protection of SCADA communications, system-level requirements, and a general plan for testing equipment.

On April 9, 2007, the U.S. Department of Homeland Security (DHS) issued the Chemical Facility Anti-Terrorism Standards (CFATS). Under Section 550 of the Department of Homeland Security Appropriations Act of 2007, Congress directed DHS to identify, assess, and ensure effective security at high-risk chemical facilities. Under CFATS, DHS requires that chemical facilities conduct a security vulnerability assessment (SVA) and then develop and implement a Site Security Plan (SSP) implementing security measures that meet the Risk Based Performance Standards (RBPS). The RBPS addresses both physical and cyber security measures. Some companies in the oil and gas sector are required to meet these standards.

QUESTION FROM CHAIRMAN DINGELL

Q6. Do you think legislation is necessary to address potential cyber security attacks on these other energy production and pipeline systems?

A6. The Administration will examine what additional authorities, if any, are appropriate for DOE to address potential cyber security attacks on other energy production and pipeline systems.

QUESTION FROM CHAIRMAN DINGELL

Q7. The Canadian Electricity Association has submitted a written statement on this hearing's topic to the subcommittee (attached). Have you discussed cyber security vulnerabilities to the Bulk Power System with federal and provincial governmental officials in Canada? If so, what has been their response to proposed cyber security emergency requirements for the Bulk Power System initiated by the U.S. Government and which could affect their sovereignty?

A7. The Department of Energy has not held discussions with the federal and provincial governmental officials in Canada specifically on emergency requirements cyber security for the Bulk Power System in North America. However, Natural Resources Canada has participated in the development of the *Roadmap to Secure Control Systems in the Energy Sector*. If DOE was authorized to implement emergency cyber security actions, DOE would most assuredly consult with the Canadian government and provide due respect to the various jurisdictional sovereignties.

QUESTION FROM CHAIRMAN DINGELL

Q8. Please itemize the instances when DOE's 202[c] authority under the Federal Power Act was used since January 1, 2000. When listing these events, please describe the duration of the DOE's emergency authority, the names of the entities to whom such orders were issued, and the actions ordered by DOE in each of these cases.

A8. Section 202(c) of the Federal Power Act (16 U.S.C. §824a(c)) actions:

- On December 14, 2000, a Federal Power Act section 202(c) emergency order was issued in response to the California energy crisis. The order was directed to the California Independent System Operator (CAISO) and a group of electricity generators that supplied the CAISO. The order required the generators, upon a finding by the CAISO that, on any given day, it was "unable to acquire in the market adequate supplies of electricity to meet system demand", to provide electricity to the CAISO on that day. The expiration date on that order was December 21, 2000, but it was extended until January 11, 2001. Due to the expiration of the December 14, 2000 order, a new order with the same terms was issued on January 11, 2001. The expiration date on that order was January 18, 2001, but it was extended until February 7, 2001, at which time the order expired.
- On August 16, 2002, due to concerns regarding the availability of electricity on Long Island in the State of New York, a 202(c) order was issued directing Cross-Sound Cable Company to operate the Cross-Sound Cable from Connecticut to Long Island and related facilities. The order expired on October 1, 2002, pursuant to its terms.

- On August 14, 2003, in response to the blackout on that day in the Northeast and Upper Midwest areas of the United States, as well as portion of Canada, the New York Independent System Operator and ISO New England were directed to require Cross-Sound Cable Company to operate the Cross-Sound Cable and related facilities. The expiration date on that order was September 1, 2003, but on August 28, 2003, it was extended "until such time as the emergency identified in the order ceases to exist." An order terminating the emergency order was issued on May 7, 2004.
- On August 24, 2005, in response to a decision by Mirant Corporation to cease generation of electricity at its Potomac river generating station, the District of Columbia Public Service Commission requested that the Secretary of Energy issue a 202(c) emergency order requiring the operation of the Potomac River generating station in order to ensure compliance with reliability standards for the central D.C. area. After investigation, the Secretary made a determination that without the operation of the Potomac River generating station there was a reasonable possibility an outage would occur that would cause a blackout in the central D.C. area. Therefore, on December 20, 2005, a 202(c) emergency order was issued requiring Mirant to operate the Potomac River generating station. The expiration date on that order was October 1, 2006, but it was extended until February 1, 2007. On January 31, 2007, a new 202(c) emergency order was issued to Mirant with substantially the same terms as the earlier order. That order expired July 1, 2007, pursuant to its terms.

- On September 14, 2008, in response to Hurricane Ike, a 202(c) emergency order was issued authorizing CenterPoint Energy to temporarily connect electricity lines to restore power to Entergy Gulf States, Inc., as well as electric cooperatives and municipal customers within the State of Texas. That order expired on November 1, 2008.
- On September 28, 2005, in response to "the massive devastation caused by Hurricane Rita, which further exacerbated the dire condition caused by Hurricane Katrina", a 202(c) emergency order was issued authorizing CenterPoint Energy to temporarily connect electricity lines to restore power to Entergy Gulf States, Inc., as well as electric cooperatives and municipal customers within the State of Texas. On September 30, 2005, also in response to Hurricane Rita, a 202(c) emergency order was issued authorizing TXU Electricity Delivery to temporarily connect and energize a line for the purposes of delivering electricity to Deep East Electric Cooperative. Both of these emergency orders expired November 1, 2005, pursuant to their terms.

RICHARD P. SERGEL, RESPONSES TO QUESTIONS FROM HON. JOHN D. DINGELL

Question No. 1: The Federal Energy Regulatory Commission (FERC) testified that 23 of 30 utilities that it audited had not complied with the June 2007 North American Electric Reliability Corporation (NERC) Advisory on the Aurora Vulnerability. To what factors do you attribute this level of compliance?

Response: NERC has not, at this time, been given access to the results of FERC's evaluation of industry efforts to comply with the mitigation measures set out in NERC's June 2007 Advisory, beyond what was discussed publicly at the September 11 hearing. Therefore, NERC is not in a position to analyze those results. Based on discussions with industry representatives, NERC believes that one important factor affecting the ability of the industry to implement mitigation measures is that industry recipients require more detailed and comprehensive engineering data on specific vulnerabilities than could be provided in NERC's Aurora Advisory. Efforts are underway to close this gap while managing the risk of disclosing a "road map" to potential adversaries.

Question No. 2: Do you believe FERC's audit results are representative of the extent of compliance by most utilities with the NERC Advisory?

Response: As stated in the response to question number one, NERC has not, at this time, been given access to specific responses made by utilities during the FERC interview process, nor are we aware of the criteria used to determine the adequacy of implemented mitigation measures. In his testimony, Chairman Kelliher described a detailed interview process by FERC staff with a sampling of geographically dispersed utilities of different sizes across the contiguous 48 states. We have no reason to believe that the results of that process are not likely to be representative of the extent of compliance by most utilities with the Aurora mitigation measures.

Question No. 3: FERC indicated that some utilities which had complied with the NERC Advisory were still vulnerable to Aurora. Please explain whether the NERC Advisory was inadequate to fully guide utilities in mitigating the Aurora Vulnerability. Please explain whether NERC has modified its advisory to address any deficiencies?

Response: The Aurora mitigation measures included in NERC's Advisory were assembled through a process that included researchers involved in the government's vulnerability demonstration project and industry subject matter experts. Clear challenges were presented in the need to utilize only information approved for distribution and the identification of measures that could be applied to a variety of different cases and unique settings. Industry recipients generally report that they require more detailed and comprehensive engineering data on specific vulnerabilities than was provided in NERC's Aurora Advisory in order to fully address a vulnerability. NERC has not, at this time, received additional information from the Federal government regarding the properties of the vulnerability or on any threat intent on exploiting the vulnerability. Consequently NERC is not, at this time, in a position to modify the Advisory.

Question No. 4: Who should have authority to implement emergency requirements: the Department of Energy or FERC?

Response: As I testified at the September 11 hearing, NERC supports legislation granting the U.S. federal government authority to act immediately in the event of an imminent cyber security threat. NERC has a strong working relationship with both the Department of Energy and the FERC. Under the Energy Policy Act of 2005, FERC certified NERC as the Electric Reliability Organization to develop and enforce mandatory reliability standards to protect and improve the reliability of the bulk power system. NERC works closely with FERC in implementing the statutory mandate. NERC also works closely with the Department of Energy, as the Sector Specific Agency for Energy, in the execution of NERC's responsibilities as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). NERC was designated as the electricity sector coordinator for critical infrastructure protection and has served in that role for several years. The agency assigned responsibility for acting in emergency situations should consult with NERC and industry experts to the maximum extent feasible in carrying out any emergency authority.

Question No. 5: How effective have Canadian utilities been in complying with the NERC Advisory on the Aurora Vulnerability? Has there been a governmental audit of compliance in Canada similar to that conducted by FERC on the Aurora Vulnerability?

Response: Canadian entities participate in NERC committees including the Critical Infrastructure Protection Committee (CIPC), and also receive information from

the ES-ISAC. When the Advisory was sent to NERC-registered Canadian entities the Canadian Electricity Association (CEA) requested and was granted permission to post the Advisory and the attached questionnaire on CEA's secure Intranet for CIP with a request that organizations review and complete it as appropriate. We are told that this was to ensure a broader dissemination of the Advisory because a limited number of Canadian organizations were on the distribution list to which the Advisory was sent directly.

Based on our discussions with Canadian utilities and Canadian government officials, NERC understands that when information about the preliminary results of the Idaho National Laboratory simulation was brought to the attention of the Canadian Cyber Incident Response Centre of Public Safety Canada, the Centre met with other government agencies with responsibility in the area to determine appropriate action. It was decided that the Energy Infrastructure Protection Division of Natural Resources Canada should arrange a meeting with energy and utilities stakeholders. In March 2007 a detailed briefing was convened for Canadian energy interests including electricity, oil and gas, and nuclear. Officials from Public Safety Canada, Natural Resources Canada, the RCMP and the Integrated Threat Assessment Centre participated and disseminated the DHS warning and information package. There was also a briefing of Canadian utility participants by staff from the Idaho National Laboratory. Industry participants had security clearances and received a confidential briefing that they say helped them understand the nature of the problem and the appropriate action to take.

The Advisory and identification and mitigation of vulnerabilities were subsequently discussed at two CEA Security and Critical Infrastructure Committee meetings. In addition, there were further contacts between Canadian government officials and DOE and DHS. Public Safety Canada advises that they coordinated actions with DHS, including the provision of sector briefings, technical advice, analysis activities at Idaho National Laboratory, and public communications strategies. To NERC's knowledge, no audit has been undertaken by Canadian government agencies of actions taken by utilities.

American
Public Power
Association

Ph: 202.467.2900
Fax: 202.467.2910
www.APPAnet.org

1875 Connecticut Avenue, NW
Suite 1200
Washington, DC 20009-5715

Responses to the Following Questions Posed to Susan N. Kelly, Vice President of Policy Analysis and General Counsel, American Public Power Association (APPA)
October 30, 2008

The Honorable John D. Dingell

1. **If the President is authorized through legislation to declare a cyber security emergency with respect to the bulk power system, which official should have the authority to trigger emergency powers? Should it be delegated? If so, to whom?**

The draft legislation supported by the electric utility industry's trade associations[1] allows the President to declare a cyber security emergency directly, or to do so through the Secretary of Energy.

2. **In the event of a national security emergency, which officials should be consulted as part of an assessment? How much time should be allotted for such consultations?**

Assuming that the phrase "national security emergency" in this question relates to cyber security threats, each of the following federal agencies has a role in assuring the cyber security of electric system assets: the Department of Energy (DOE), which in addition to its expertise in energy, security, and electric system matters serves as the "Sector Specific Agency" for the electric industry "Sector Coordinating Council" under the federal "National Infrastructure Protection Plan," and has worked closely with the electric sector in developing the "Energy Sector Specific Plan"; the Federal Energy Regulatory Commission (FERC), with its responsibility for regulating bulk power system (BPS) reliability; the Department of Homeland Security (DHS), which has ultimate responsibility for implementing the National Infrastructure Protection Plan; and possibly the Department of Defense (DOD). Since U.S. electric utilities operate within an interconnected network that encompasses Canada and northern Mexico, governmental counterparts in Canada and Mexico should also be consulted.

Because any actions ordered in such an emergency would likely have adverse consequences for reliability and would therefore need to quickly be replaced by more sustainable measures, such as reliability standards, the Associations believe that a representative group of informed electric utility industry personnel must also be consulted as quickly as possible. The North American Electric Reliability Corporation (NERC) has recently set up a small group of industry executives, the Electricity Sector Steering Group (ESSG), to serve as a resource and source of advice on

[1] The American Public Power Association, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group (Associations).

critical infrastructure protection issues. These executives have at their disposal many technical resources within NERC, including the NERC Critical Infrastructure Protection Committee and that committee's Executive Committee, which worked closely with technical experts at DOE to develop the Energy Sector Specific Plan. Since NERC serves as the Electric Sector Information Sharing and Analysis Center (ES-ISAC), it should be consulted as well.

In the case of non-cyber-related national security emergencies, the Associations believe that existing statutory authorities providing for coordination, information sharing and analysis between federal agencies and the private sector are sufficient to address national security threats and vulnerabilities that are made known to the electric utility industry. Improvements to the coordination process and to the sharing of clear, timely, actionable threat information with industry are needed, but these steps do not require additional statutory authority. Further, as outlined in Mr. Sergel's September 11 testimony, NERC has undertaken steps to improve current procedures for alerting targeted entities in the electric utility industry about potential threats and vulnerabilities. The electric utility industry is working with NERC to ensure that these procedures will work in practice when they are needed, so that actionable information actually reaches the individual business units and employees responsible for taking steps to address such threats.

The time allotted for such consultations must by necessity be determined by the nature of the threat, and the timeline for its possible occurrence. This is why the draft legislation stated in Section 215A(c)(2) that FERC would consult with appropriate governmental authorities in Canada and Mexico, users, owners and operators of the BPS in the United States, and officials at other federal agencies "to the extent feasible, taking into account the nature of the threat and the urgency of need for action." In some cases, the consultation process may require less than 24 hours. In other cases, where remedial measures may require installation of new hardware or software that could interact with existing systems in unforeseen ways, the consultation process may require days or even weeks, to ensure that government directives do not jeopardize reliable bulk power system operations.

The Honorable Edward J. Markey

1. The industry organizations, and your testimony in particular, strongly assert the need to ensure that any legislation ultimately enacted to provide additional authority to FERC is carefully crafted to limit that additional authority to only address cyber-security threats, and not to provide authority to address the broader national security concerns that Chairman Kelliher reported is necessary. During the hearing, when Chairman Kelliher was asked to describe a non-cyber security national threat that might require the kind of immediate response most often linked to cyber threats he provided a couple of examples, including: 1) ordering spare transformers to be moved to other locations or 2) ordering generators to have more power on-call in the event other generators go off-line. Do these examples change your opinion about the need for the expanded breadth of the draft legislation? Why or why not? If the concern is the vague language currently within the draft legislation, what alternate language do you believe would allow for non-cyber national security threats but more concisely capture the appropriate scope of events covered?

The Associations are still of the opinion that any legislation should be limited to cyber-security threats, and should not be expanded to include "other national security threats." As I explained and as was echoed by Mr. Naumann and Mr. Lawson at the hearing, non-cyber-related threats to electric systems have been encountered for many years. Electric utility systems work with state and local law enforcement, the Federal Bureau of Investigation, and other appropriate federal law enforcement agencies, such as the Defense Security Agency (when related to defense facilities), to address such threats. The Associations therefore do not believe that additional statutory authorities are needed in this area; nor have any federal law enforcement agencies articulated to industry that there is a need for additional authority and why.

Threats to the nation's critical infrastructures often cut across industry sectors, as well as the authorities, expertise and jurisdiction of various government agencies. For example, a chemical security threat may require action by one or more of the electric, telecommunications, chemical, mining, oil and gas, industrial manufacturing, railroad and/or water utility industries – depending on the nature of the threat. The electric utility industry has worked closely with government agencies and industry organizations to deal with cross-sector threats such as the Y2K issue and the aftermath of 9/11. The industry has a strong track record of working with government agencies such as DOE, DOD, DHS, the Federal Emergency Management Agency and NERC to prepare for and restore electric service after catastrophic events such as hurricanes. In some cases, it can be a utility or other industry entity that identifies a national security-related problem or concern and notifies local, state and/or federal law enforcement or other appropriate authorities.

The two examples provided do not merit specific legislation to address them. Electric utilities have very extensive past experience preparing for and responding to many types of emergencies on their systems. They have in place many programs and systems for sharing equipment, personnel, and other resources with other utilities. Government attempts to respond to an actual or potential national security threat by ordering specific utility actions could be inadvertently focused on the wrong actions, without necessarily addressing significant impediments to utility action. For example, in some cases where crews or equipment need to be moved quickly in response to an emergency, impediments can arise from factors largely outside electric utilities' control (and beyond the expertise of FERC), such as state and federal highway regulations that require pre-approval of routes, the need for law enforcement escorts, etc., or rail capacity constraints that can complicate movements of large transformers.

Moreover, the industry deals routinely with generator outages for both routine maintenance and unscheduled events. Entities known as "reliability coordinators" are responsible for monitoring regional transmission system operations, and ensuring that sufficient generation is available to support reliable system operations.

The role proposed for FERC in the draft legislation in dealing with cyber-security threats has a close nexus to its existing role under Federal Power Act Section 215 to approve and enforce mandatory reliability standards for the BPS. FERC's responsibility to ensure protection of the BPS from cyber-security threats is expressly provided in Section 215. Indeed, to the extent that other federal government agencies are given authority to direct the electric utility industry to take

measures to protect against cyber-security threats, conflicts with cyber-security-related mandatory reliability standards developed by NERC and approved by FERC are likely to occur. In marked contrast, other national security threats to the electric utility industry are likely to involve numerous other federal, state and local agencies, particularly in areas of public security and safety.

Because the Associations do not support expanding any legislation drafted to deal with cyber security issues to deal with non-cyber threats, I am not proposing specific statutory language in this area.

I also note that my answer to Chairman Dingell's question No. 2 above is relevant to this question.

2. **Your testimony also argues for retaining the draft legislation's limited jurisdiction to that of bulk power systems as defined in the Federal Power Act. As we have learned, this means that states like Alaska and Hawaii would not be covered by this expanded authority, nor would many major metropolitan areas, or distribution system that carry this electricity into our homes. With the seemingly unanimous recognition among industry groups of the growing and alarming threat of cybersecurity on our nation's grid. [sic] And the impacts of any such incident ultimately, through economic impacts or the threat to health and safety, fall to the consumers of electricity. If FERC's authority is limited to the bulk power system, how then do we protect those in Alaska, or Hawaii or our distribution system, from this same real threat?**

The electric grids of the states of Alaska and Hawaii are completely isolated from those in the remainder of the United States. State public utility commissions (PUCs) regulate the investor-owned utilities providing service in those states. The electric systems in these two states are best thought of as a series of individual grids with only weak interconnections, even within each state. Therefore, an outage caused by a cybersecurity incident does not have the same potential to "cascade" into a large outage adversely affecting many millions of customers, as happened in the Northeast in August 2003. These electric systems are also often configured very differently than those in the mainland U.S.; for example, in some instances there is much more reliance on fuel oil as a generation fuel, because natural gas, coal and nuclear options are often not available. Since the Alaska and Hawaii PUCs are both geographically close to and well familiar with the specific characteristics of these systems, it makes sense to defer to them. Additionally, there is no reason why DOE or FERC could not communicate directly with these states if the Secretary of Energy has information that a cyber security threat could adversely impact them.

In particular, the Secretary of Energy has established an "Office of Infrastructure Security and Energy Restoration" that could be tasked to perform this federal-state program coordination function. This DOE office is responsible for supporting the national critical infrastructure program, analyzing infrastructure vulnerabilities and recommending preventive actions, and conducting emergency energy operations during a declared emergency or national security special event in accordance with the "National Recovery Plan."

The Associations are aware that the Committee is especially concerned about reliability of service to military installations in these states. The Associations agree that it would be appropriate for the electric utilities in Alaska and Hawaii serving military installations to confer with the responsible personnel at the installations they serve and if necessary, with DOE and DOD, on possible steps to ensure continued reliable service to those facilities in the face of increased cybersecurity threats. We believe, however, that it is not necessary for such utilities to file formal plans with FERC.

Much the same analysis applies to local distribution systems in the lower 48, even those in major metropolitan areas. State PUCs and other state/local regulatory authorities have long dealt with distribution service reliability issues. These authorities are well versed in local system characteristics and conditions, which differ substantially from those of the interstate transmission grid.[2] Moreover, local distribution systems vary widely in their specific configurations and designs, so that state and local officials are best positioned to take the necessary protective steps. And again, there is no reason why DOE or FERC could not communicate directly with these states if the Secretary of Energy has information that a cyber security threat could adversely impact distribution systems within their borders.

[2] In Section 215(i)(3) of the Federal Power Act, Congress specifically preserved the authority of States to ensure the reliability of electric service within their states, so long as their actions were not inconsistent with mandatory reliability standards implemented under Section 215. In fact, the State of New York was given the express authority to establish rules resulting in *greater* reliability within New York than the federal standards would require.

Exelon

Exelon Corporation
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001

www.exeloncorp.com

October 30, 2008

The Honorable John D. Dingell
Chairman
Committee on Energy and Commerce
United States House of Representatives
2322-B Rayburn HOB
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter seeking my response to further questions for the record in relation to the Subcommittee on Energy and Air Quality's hearing entitled "Protecting the Electric Grid from Cyber-Security Threats" held on September 11, 2008. Please find attached my responses to those questions.

I commend you and the Committee on your efforts on this important matter. As the Committee continues its work on this issue, please do not hesitate to call on me if you have any further questions.

Sincerely,

Steven T. Naumann

Steven T. Naumann
Vice President, Wholesale Market Development

cc: The Honorable Joe Barton
Ranking Member

Questions from Chairman Dingell

1. Was Exelon one of the companies interviewed by Federal Energy Regulatory Commission (FERC) regarding compliance with the North American Electric Reliability Corporation (NERC) Advisory on the Aurora vulnerability?

A. Yes.

2. Are Exelon facilities 100 percent compliant with the NERC advisory? If not, how far along is Exelon in coming into compliance with the immediate and interim mitigation requirements?

A. Exelon believes it is 100% compliant but has not received explicit feedback from FERC Staff as to whether FERC Staff believes that to be true.

3. Your testimony stated that, based on conversations with peer companies, you believe that other utilities have responded in an appropriate fashion to the NERC advisory. However, FERC's audit found that only 23 out of 30 were in full compliance with the Advisory. For example, one major utility had apparently taken no action to comply with the Advisory other than prepare for the FERC interview. Others had only protected a small subset of their vulnerable equipment, and one company had a 10-year compliance schedule. In your opinion, is this a sufficient response from the industry?

A. I did not mean for my testimony to be taken or interpreted as a definitive summary of peer companies' response to the NERC advisory. Rather it was a very informal assessment of their response based upon my informal conversations with my peers involved in the NERC process. I do not have adequate information to have an informed opinion about whether FERC staff determinations of compliance/noncompliance are consistent with NERC expectations regarding individual utility responses to the Aurora Advisory. Only FERC is in a position to provide the Subcommittee with a definitive picture. We believe that more expansive, definitive feedback from FERC is appropriate, including lessons learned and proposed steps forward, subject to appropriate confidentiality provisions.

4. As you know, FERC found that utilities installed internet-linked controls, but never changed the factory provided usernames and passwords, which seems like a fairly basic measure. How extensive are vulnerabilities like these in the industry?

A. I have not seen the FERC findings nor do I not know the extent of these vulnerabilities throughout the entire industry. Exelon's policy with respect to internet-linked controls is to use strong passwords and to change those passwords periodically.

5. Does a smart grid invite cyber security problems? Who should establish cyber standards for smart grid technology?

A. While I have no personal expertise in smart grid technology, Exelon believes that development and deployment of smart grid technology is very important and, in the process of doing so, we must address any cyber security issues. In the Energy Independence and Security Act (EISA) of 2007, Congress addressed who should establish a framework for protocols and standards for cyber security and other elements of smart grid functionality and interoperability. We support the division of labor established therein.

6. The NERC Critical Infrastructure Protection Standards exclude nuclear plants regulated by the Nuclear Regulatory Commission (NRC). According to FERC, there were cyber incidents involving the Browns Ferry and Hatch nuclear power plants. Are there any gaps between FERC and NRC authority with respect to cyber security protections?

A. The question as to whether or not there is a regulatory gap between FERC and NRC authority is currently being explored by FERC in an inquiry on proposed clarification. 73 Fed. Reg. 55,459 (Sept. 15, 2008). Comments are due November 3, 2008.

7. What is Exelon's cost of compliance with mitigating the Aurora vulnerability? How will these costs differ from the forthcoming NERC standards for cyber security?

A. The costs incurred by the Exelon Companies, Commonwealth Edison Company, Exelon Generation LLC and PECO Energy, in complying with the Aurora Advisory were approximately $1.2 million. Exelon's estimated costs to comply with the existing NERC Standards for cyber security are $11 million through 2010. This estimate does not include ongoing costs of compliance or compliance with any new or revised NERC Standards.

Questions from Cong. Markey

1. There was a suggestion at the hearing that one way to address the cyber-security of the grid system beyond that of the bulk power system would be through a consultation process. If the cyber threat to the bulk power system demands an increased federal authority in order to permit an immediate response to any security incident or threat thereof, how would a consultation process provide the same level of protection for those on the grid beyond the bulk power system? If it would not, why is it appropriate to settle for only limited protection of the grid?

A. In general, the most effective way to design critical infrastructure (including cyber) protection and remediation measures is in consultation with owner-operators of that critical infrastructure. As outlined in my testimony, owners, users, and operators of the bulk power system are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation. A consultative process to address cyber security vulnerabilities and threats should result in better—not more limited—protection of the grid.

The interconnected nature of the bulk power system lends itself to a more centralized and uniform approach to cyber security standards and remediation. In contrast, portions of the grid beyond the bulk power system (i.e., distribution systems) are much more diverse. There are significant differences in design among different local utilities, and often even among different areas served within each utility distribution system. This multiplies the complexity and difficulty—and the potential cost—of effectively addressing cyber security issues at the distribution level through "one-size-fits-all" federal requirements. Designing protections or remediation measures for distribution systems in consultation with distribution utilities and state and local regulatory authorities will result in more effective protection, not less.

4. This Congress has heard hours of testimony on some pressing grid issues and some promising grid solutions, including those centered around "smart grid" technology. In your testimony you spoke of the promising future of smart grids. Moreover, you offered testimony regarding the need to ensure that whatever grid solutions we implement in the smart grid realm appropriately capture cyber security protections. I am glad to hear the industry's recognition of the importance of integrating policy, practice and technology in this emerging field. Could you provide me with specific examples of how the industry is working toward the goal of ensuring appropriate integration in the developing field of smart grid technology? If not, can you explain why not and what would need to happen to have a more integrated approach pursued?

A. First, I refer to my answer to Question 5 from Chairman Dingell for a description of the process by which smart grid security issues are being

addressed pursuant to EISA 2007. Within Exelon, as we develop our own smart grid strategies, Information Technology is intimately involved. Cyber security requirements are something that are thoughtfully being included in our strategies and designs.

BARRY R. LAWSON, RESPONSES TO QUESTIONS FROM HON. EDWARD J. MARKEY

Question No. 1: There was a suggestion at the hearing that one way to address the cyber-security of the grid system beyond that of the bulk power system would be through a consultation process. If the cyber threat to the bulk power system demands an increased federal authority in order to permit an immediate response to any security incident or threat thereof, how would a consultation process provide the same level of protection for those on the grid beyond the bulk power system? If it would not, why is it appropriate to settle for only limited protection of the grid?

Response:

A consultation process is appropriate regarding electric system facilities that are beyond the bulk power system. These facilities are in most cases considered to be the distribution system. The bulk power system is significantly different from the distribution system. There are clear reasons why these distribution facilities should not be treated the same as the bulk power system in cyber security legislation.

• Giving FERC or any other federal agency jurisdiction over the distribution elements of the electric utility system causes complications with state and local regulatory authorities.

o Most distribution facilities are beyond the jurisdiction of FERC. The FPA expressly reserves jurisdiction over distribution facilities to the states.

o The regulation of the distribution system is imbued with a number of local economic and political issues that are best handled at the local level, not the federal level.

o FERC is not as familiar and will never be as familiar as the individual states are with the structure and design of the local distribution system in their states.

o State PUCs and other state/local regulatory authorities have traditionally dealt with distribution service reliability issues. These authorities best understand local distribution system characteristics and conditions, which differ substantially from those of the bulk power system. Local distributions systems vary widely in their specific configurations and designs, making utilities and state/local officials best positioned to take protective steps when necessary.

• When comparing the bulk power system to the distribution system, it is important to understand several distinctions.

o An incident on the bulk power system can potentially impact a larger geographical area and a corresponding potential larger number of consumers. An incident on the distribution system impacts a smaller area and a lesser number of consumers. That means protection of the bulk power system is a higher priority for the electric utility industry, and that the distribution system will pose a much lower priority target.

o Distribution facilities are typically quicker and easier to restore than bulk power system facilities. A distribution circuit can often be easily restored merely by replacing a single failed element and then re-energizing the circuit. Restoring the bulk power system, however, is much more complicated. Because of the large number of components and integrated network nature of the bulk power system, it can require significant regional coordination and considerable time for re-energizing.

o Many distribution system elements are not automated/controlled remotely with programmable devices and therefore not necessarily vulnerable to cyber issues.

o The distribution system is separated from the bulk power system through protection protocols and equipment.

• Distribution circuits fail without any cyber attacks. Automobile accidents and animal-related interruptions are some of the most common causes of outages and they cannot be completely prevented. Utilities have a long history of successfully demonstrating that they are well-prepared to respond to these and other incidents on their distribution system.

• Because of these differences, the distribution system does not require the same level of protection as the bulk power system.

o Where an uncontrolled failure of the bulk power system can potentially lead to a "cascading" failure potentially affecting a large number of consumers, an uncontrolled failure of a distribution circuit is unlikely to affect a large number of consumers and is limited to those consumers on a particular distribution circuit.

o Distribution circuits are seldom material to the reliability of the bulk power system and, when they are material, they currently fall within the definition of the bulk power system.

• Accordingly, with the preceding information being understood, it is not necessary or appropriate, and can in fact be disruptive, for distribution facilities to be addressed in a similar manner as bulk power system facilities.

Question No. 2: This Congress has heard hours of testimony on some pressing grid issues and some promising grid solutions, including those centered around "smart grid" technology. Your testimony reported that in 2006, cooperatives lead the industry in installation of smart meters. Moreover, you offered testimony regarding the need to ensure that whatever grid solutions we implement in the smart grid realm appropriately capture cyber security protections. I am glad to hear both the progress demonstrated by the cooperatives with smart grid initiatives and the industry's recognition of the importance of integrating policy, practice and technology in this emerging field. Can you provide me with specific examples of how the industry is working toward the goal of ensuring appropriate integration in the field of smart grid technology? If not, can you explain why not and what would need to happen to have a more integrated approach pursued?

Response:

• "Smart Grid" technology often uses the internet and other automated equipment. Therefore, it is potentially vulnerable to cyber issues. Implementation of this technology should always include cyber protection related to the equipment/devices that are being utilized.

• Cyber security should be a part of an entity's due diligence when considering the use of such technology. I understand that this is addressed by entities when they consider using "smart grid" technology.

○