AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING THE ELECTRIC GRID: H.R. ———, THE GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY AND POWER

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 31, 2011

Serial No. 112–52

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

72–383 PDF WASHINGTON : 2012

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

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chair
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands

SUBCOMMITTEE ON ENERGY AND POWER

ED WHITFIELD, Kentucky
Chairman

JOHN SULLIVAN, Oklahoma
Vice Chairman
JOHN SHIMKUS, Illinois
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MICHAEL C. BURGESS, Texas
BRIAN P. BILBRAY, California
STEVE SCALISE, Louisiana
CATHY McMORRIS RODGERS, Washington
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
H. MORGAN GRIFFITH, Virginia
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

BOBBY L. RUSH, Illinois
Ranking Member
JAY INSLEE, Washington
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDWARD J. MARKEY, Massachusetts
ELIOT L. ENGEL, New York
GENE GREEN, Texas
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHARLES A. GONZALEZ, Texas
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Ed Whitfield, a Representative in Congress from the Commonwealth of Kentucky, opening statement	1
Prepared statement	3
Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	29
Hon. Henry A. Waxman, a Representative in Congress from the State of California, opening statement	30
Hon. Fred Upton, a Representative in Congress from the State of Michigan, prepared statement	152

WITNESSES

Hon. Trent Franks, a Representative in Congress from the State of Arizona	31
Prepared statement	34
Hon. James R. Langevin, a Representative in Congress from the State of Rhode Island	44
Prepared statement	46
Patricia A. Hoffman, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, Department of Energy	52
Prepared statement	54
Additional comments (for Mr. McKinley)	90
Additional comments (for Mr. Olson)	100
Paul N. Stockton, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, Department of Defense	60
Prepared statement	62
Joseph H. McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission	72
Prepared statement	74
Additional comments	96
Gerry Cauley, President and CEO, North American Electric Reliability Corporation	103
Prepared statement	106
Franklin D. Kramer, former Assistant Secretary of Defense for International Security Affairs, Department of Defense	121
Prepared statement	123
Barry R. Lawson, Associate Director, Power Delivery and Reliability, National Rural Electric Cooperative Association	132
Prepared statement	134

SUBMITTED MATERIAL

Discussion Draft of H.R. ————, To amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities	7

PROTECTING THE ELECTRIC GRID: H.R. ———, THE GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT

TUESDAY, MAY 31, 2011

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

The subcommittee met, pursuant to call, at 2:07 p.m., in room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (chairman of the subcommittee) presiding.

Members present: Representatives Whitfield, Terry, Burgess, Scalise, McMorris Rodgers, Olson, McKinley, Pompeo, Rush, Markey and Waxman (ex officio).

Staff present: Maryam Brown, Chief Counsel, Energy and Power; Allison Busbee, Legislative Clerk; Patrick Currier, Counsel, Energy and Power; Greg Dotson, Democratic Energy and Environment Staff Director; and Caitlin Haberman, Democratic Policy Analyst.

OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. WHITFIELD. I call this hearing to order. The hearing is entitled "Protecting the Electric Grid: the Grid Reliability and Infrastructure Defense Act."

Today's hearing focuses on protecting the Nation's electric grid from physical and cybersecurity threats and vulnerabilities. A secure grid is of utmost importance to our national security, of course, and our national economic interests.

Cybersecurity threats and vulnerabilities to the electric grid have increased in recent years and were the subject of several hearings in the 110th and 111th Congresses. There is evidence that bad actors have conducted cyber probes of U.S. grid systems, and that cyber attacks have been conducted against critical electric infrastructure in other countries.

This past February, a cyber attack dubbed Night Dragon, which is believed to have emanated from China, targeted the critical infrastructure of energy and petrochemical companies in the United States. The Night Dragon attack was not overly sophisticated, but was nevertheless successful in breaching the computer systems of key assets. This example is one of several, and is the tip of the iceberg, and illustrates that we must be more vigilant in securing the Nation's critical energy infrastructure, including the electric grid.

Beyond potential cyber attacks, the bulk power system remains exposed to physical vulnerabilities and threats, including direct terrorist attacks, weapons that can create an electromagnetic pulse, and geomagnetic storms. Federal and State agencies and industry stakeholders have sought to address many of these concerns. In particular, through an extensive stakeholder process, the North American Electric Reliability Corporation, pursuant to its authority under section 215 of the Federal Power Act, has worked over the last several years to develop and implement reliability standards and to address grid security vulnerabilities in a timely manner.

To address these shortcomings, the Committee recently released a discussion draft entitled the "Grid Reliability and Infrastructure Defense Act" or the GRID Act. The bill is identical to bipartisan legislation developed by this committee last Congress by Chairman Upton and Mr. Markey. The GRID Act provides the Federal Energy Regulatory Commission with emergency authority to respond to imminent physical and cyber threats to the bulk power system and electric infrastructure that serves facilities vital to our national defense. This emergency authority can be triggered only upon a directive from the President. The discussion draft also provides FERC with authority to identify and remedy weaknesses that leave the grid vulnerable to cyber attacks and electromagnetic pulse events. Notably, the legislation also directs FERC to develop regulations to facilitate the sharing of information, as appropriate, between governmental agencies, NERC, and owners and operators of the bulk power system. Doing so will improve communication among affected stakeholders, which will result, we hope, in a more secure grid.

Although the discussion draft is identical to last year's bill, we expect that input from today's witnesses and insight provided by those witnesses will help us improve the bill to reflect current conditions and any changed circumstances. I know, for example, that Congressman Franks has introduced legislation that is, I believe, more narrowly focused than this broader approach, and we look forward to his testimony to explain his views on this area because he has spent a great deal of time on it, as has Congressman Langevin.

So I want to thank the witnesses in advance for being with us today. I will introduce them a little bit later.

[The prepared statement of Mr. Whitfield follows:]

Opening Statement of the Honorable Ed Whitfield
Chairman, Subcommittee on Energy and Power
Committee on Energy and Commerce
Hearing entitled "Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act"
May 31, 2011

- Today's hearing focuses on a critical national security issue – protecting the nation's electric grid from physical and cybersecurity threats and vulnerabilities.

- A secure grid is of utmost importance to our national security and our national economic interests. The grid is vital to all aspects of American life. The daily lives of all Americans are powered by electricity provided by the electric grid, the disruption of which would cut off the supply of electric power to our homes, hospitals, schools, offices, farms and factories.

- Cybersecurity threats and vulnerabilities to the electric grid have increased in recent years and were the subject of several hearings in the 110th and 111th Congresses. There is evidence that 'bad actors' have conducted cyber 'probes' of U.S. grid systems, and that cyber attacks have been conducted against critical electric infrastructure in other countries.

- This past February, a cyber attack dubbed "Night Dragon," which is believed to have emanated from China, targeted the critical infrastructure of energy and petrochemical companies. The Night Dragon attack was not overly sophisticated, but was nevertheless successful in breaching the computer systems of key assets.

- This example is one of several, and is the tip of the iceberg, and illustrates that we must be more vigilant in securing the nation's critical energy infrastructure, including the electric grid.

- Beyond potential cyber attacks, the bulk power system remains exposed to physical vulnerabilities and threats, including direct terrorist attacks, weapons that can create an electromagnetic pulse, and geomagnetic storms.

- Federal and state agencies and industry stakeholders have sought to address many of these concerns. In particular, through an extensive stakeholder process, the North American Electric Reliability Corporation (NERC), pursuant to its authority under Section 215 of the Federal Power Act, has worked over the last several years to develop and implement reliability standards and cybersecurity infrastructure protection standards.

- Many believe, however, that the NERC process could be improved for responding to imminent threats and to address grid security vulnerabilities in a timely manner.

- To address these shortcomings, the Committee recently released a discussion draft entitled the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act." The bill is identical to bipartisan legislation developed by this Committee last Congress by Chairman Upton and Mr. Markey.

- The GRID Act arms the Federal Energy Regulatory Commission (FERC) with emergency authority to respond to imminent physical and cyber threats to the bulk power system and electric infrastructure that serves facilities vital to our national defense. This emergency authority can be triggered only upon a directive from the President.

- The discussion draft also provides FERC with authority to identify and remedy weaknesses that leave the grid vulnerable to cyber attacks and electromagnetic pulse events.

- Notably, the legislation also directs FERC to develop regulations to facilitate the sharing of information, as appropriate, between governmental agencies, NERC, and owners and

operators of the bulk power system. Doing so will improve communication among affected stakeholders, which will result in a more secure grid.

- Although the discussion draft is identical to last year's bill, we expect that input and insight provided by today's witnesses will help us improve the bill to reflect current conditions and any changed circumstances.

- I thank the witnesses for being here today and look forward to the discussion.

- With that I yield to the Ranking Member, Mr. Rush.

[H.R. ———— follows:]

[DISCUSSION DRAFT]

112TH CONGRESS
1ST SESSION

H. R. _____

To amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities.

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 "Grid Reliability and Infrastructure Defense Act" or the "GRID Act".

1 **SEC. 2. AMENDMENT TO THE FEDERAL POWER ACT.**

2 (a) CRITICAL ELECTRIC INFRASTRUCTURE SECU-
3 RITY.—Part II of the Federal Power Act (16 U.S.C. 824
4 et seq.) is amended by adding after section 215 the fol-
5 lowing new section:

6 **"SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECU-**
7 **RITY.**

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

9 "(1) BULK-POWER SYSTEM; ELECTRIC RELI-
10 ABILITY ORGANIZATION; REGIONAL ENTITY.—The
11 terms 'bulk-power system', 'Electric Reliability Or-
12 ganization', and 'regional entity' have the meanings
13 given such terms in paragraphs (1), (2), and (7) of
14 section 215(a), respectively.

15 "(2) DEFENSE CRITICAL ELECTRIC INFRA-
16 STRUCTURE.—The term 'defense critical electric in-
17 frastructure' means any infrastructure located in the
18 United States (including the territories) used for the
19 generation, transmission, or distribution of electric
20 energy that—

21 "(A) is not part of the bulk-power system;
22 and

23 "(B) serves a facility designated by the
24 President pursuant to subsection (d)(1), but is
25 not owned or operated by the owner or operator
26 of such facility.

1 "(3) DEFENSE CRITICAL ELECTRIC INFRA-
2 STRUCTURE VULNERABILITY.—The term 'defense
3 critical electric infrastructure vulnerability' means a
4 weakness in defense critical electric infrastructure
5 that, in the event of a malicious act using electronic
6 communication or an electromagnetic pulse, would
7 pose a substantial risk of disruption of those elec-
8 tronic devices or communications networks, includ-
9 ing hardware, software, and data, that are essential
10 to the reliability of defense critical electric infra-
11 structure.
12 "(4) ELECTROMAGNETIC PULSE.—The term
13 'electromagnetic pulse' means 1 or more pulses of
14 electromagnetic energy emitted by a device capable
15 of disabling, disrupting, or destroying electronic
16 equipment by means of such a pulse.
17 "(5) GEOMAGNETIC STORM.—The term 'geo-
18 magnetic storm' means a temporary disturbance of
19 the Earth's magnetic field resulting from solar activ-
20 ity.
21 "(6) GRID SECURITY THREAT.—The term 'grid
22 security threat' means a substantial likelihood of—
23 "(A)(i) a malicious act using electronic
24 communication or an electromagnetic pulse, or
25 a geomagnetic storm event, that could disrupt

1 the operation of those electronic devices or com-
2 munications networks, including hardware, soft-
3 ware, and data, that are essential to the reli-
4 ability of the bulk-power system or of defense
5 critical electric infrastructure; and
6 "(ii) disruption of the operation of such
7 devices or networks, with significant adverse ef-
8 fects on the reliability of the bulk-power system
9 or of defense critical electric infrastructure, as
10 a result of such act or event; or
11 "(B)(i) a direct physical attack on the
12 bulk-power system or on defense critical electric
13 infrastructure; and
14 "(ii) significant adverse effects on the reli-
15 ability of the bulk-power system or of defense
16 critical electric infrastructure as a result of
17 such physical attack.
18 "(7) GRID SECURITY VULNERABILITY.—The
19 term 'grid security vulnerability' means a weakness
20 that, in the event of a malicious act using electronic
21 communication or an electromagnetic pulse, would
22 pose a substantial risk of disruption to the operation
23 of those electronic devices or communications net-
24 works, including hardware, software, and data, that

1 are essential to the reliability of the bulk-power sys-
2 tem.
3 "(8) LARGE TRANSFORMER.—The term 'large
4 transformer' means an electric transformer that is
5 part of the bulk-power system.
6 "(9) PROTECTED INFORMATION.—The term
7 'protected information' means information, other
8 than classified national security information, des-
9 ignated as protected information by the Commission
10 under subsection (e)(2)—
11 "(A) that was developed or submitted in
12 connection with the implementation of this sec-
13 tion;
14 "(B) that specifically discusses grid secu-
15 rity threats, grid security vulnerabilities, de-
16 fense critical electric infrastructure
17 vulnerabilities, or plans, procedures, or meas-
18 ures to address such threats or vulnerabilities;
19 and
20 "(C) the unauthorized disclosure of which
21 could be used in a malicious manner to impair
22 the reliability of the bulk-power system or of
23 defense critical electric infrastructure.
24 "(10) SECRETARY.—The term 'Secretary'
25 means the Secretary of Energy.

1 "(11) SECURITY.—The definition of 'security'
2 in section 3(16) shall not apply to the provisions in
3 this section.
4 "(b) EMERGENCY RESPONSE MEASURES.—
5 "(1) AUTHORITY TO ADDRESS GRID SECURITY
6 THREATS.—Whenever the President issues and pro-
7 vides to the Commission (either directly or through
8 the Secretary) a written directive or determination
9 identifying an imminent grid security threat, the
10 Commission may, with or without notice, hearing, or
11 report, issue such orders for emergency measures as
12 are necessary in its judgment to protect the reli-
13 ability of the bulk-power system or of defense critical
14 electric infrastructure against such threat. As soon
15 as practicable but not later than 180 days after the
16 date of enactment of this section, the Commission
17 shall, after notice and opportunity for comment, es-
18 tablish rules of procedure that ensure that such au-
19 thority can be exercised expeditiously.
20 "(2) NOTIFICATION OF CONGRESS.—Whenever
21 the President issues and provides to the Commission
22 (either directly or through the Secretary) a written
23 directive or determination under paragraph (1), the
24 President (or the Secretary, as the case may be)
25 shall promptly notify congressional committees of

1 relevant jurisdiction, including the Committee on
2 Energy and Commerce of the House of Representa-
3 tives and the Committee on Energy and Natural Re-
4 sources of the Senate, of the contents of, and jus-
5 tification for, such directive or determination.
6 "(3) CONSULTATION.—Before issuing an order
7 for emergency measures under paragraph (1), the
8 Commission shall, to the extent practicable in light
9 of the nature of the grid security threat and the ur-
10 gency of the need for such emergency measures, con-
11 sult with appropriate governmental authorities in
12 Canada and Mexico, entities described in paragraph
13 (4), the Secretary, and other appropriate Federal
14 agencies regarding implementation of such emer-
15 gency measures.
16 "(4) APPLICATION.—An order for emergency
17 measures under this subsection may apply to—
18 "(A) the Electric Reliability Organization;
19 "(B) a regional entity; or
20 "(C) any owner, user, or operator of the
21 bulk-power system or of defense critical electric
22 infrastructure within the United States.
23 "(5) DISCONTINUANCE.—The Commission shall
24 issue an order discontinuing any emergency meas-

1 ures ordered under this subsection, effective not
2 later than 30 days after the earliest of the following:
3 "(A) The date upon which the President
4 issues and provides to the Commission (either
5 directly or through the Secretary) a written di-
6 rective or determination that the grid security
7 threat identified under paragraph (1) no longer
8 exists.
9 "(B) The date upon which the Commission
10 issues a written determination that the emer-
11 gency measures are no longer needed to address
12 the grid security threat identified under para-
13 graph (1), including by means of Commission
14 approval of a reliability standard under section
15 215 that the Commission determines adequately
16 addresses such threat.
17 "(C) The date that is 1 year after the
18 issuance of an order under paragraph (1).
19 "(6) COST RECOVERY.—If the Commission de-
20 termines that owners, operators, or users of the
21 bulk-power system or of defense critical electric in-
22 frastructure have incurred substantial costs to com-
23 ply with an order under this subsection and that
24 such costs were prudently incurred and cannot rea-
25 sonably be recovered through regulated rates or

1 market prices for the electric energy or services sold
2 by such owners, operators, or users, the Commission
3 shall, after notice and an opportunity for comment,
4 establish a mechanism that permits such owners, op-
5 erators, or users to recover such costs.
6 "(c) MEASURES TO ADDRESS GRID SECURITY
7 VULNERABILITIES.—
8 "(1) COMMISSION AUTHORITY.—If the Commis-
9 sion, in consultation with appropriate Federal agen-
10 cies, identifies a grid security vulnerability that the
11 Commission determines has not adequately been ad-
12 dressed through a reliability standard developed and
13 approved under section 215, the Commission shall,
14 after notice and opportunity for comment and after
15 consultation with the Secretary, other appropriate
16 Federal agencies, and appropriate governmental au-
17 thorities in Canada and Mexico, promulgate a rule
18 or issue an order requiring implementation, by any
19 owner, operator, or user of the bulk-power system in
20 the United States, of measures to protect the bulk-
21 power system against such vulnerability. Before pro-
22 mulgating a rule or issuing an order under this
23 paragraph, the Commission shall, to the extent prac-
24 ticable in light of the urgency of the need for action
25 to address the grid security vulnerability, request

1 and consider recommendations from the Electric Re-
2 liability Organization regarding such rule or order.
3 The Commission may establish an appropriate dead-
4 line for the submission of such recommendations.
5 "(2) CERTAIN EXISTING CYBERSECURITY
6 VULNERABILITIES.—Not later than 180 days after
7 the date of enactment of this section, the Commis-
8 sion shall, after notice and opportunity for comment
9 and after consultation with the Secretary, other ap-
10 propriate Federal agencies, and appropriate govern-
11 mental authorities in Canada and Mexico, promul-
12 gate a rule or issue an order requiring the imple-
13 mentation, by any owner, user, or operator of the
14 bulk-power system in the United States, of such
15 measures as are necessary to protect the bulk-power
16 system against the vulnerabilities identified in the
17 June 21, 2007, communication to certain 'Electricity
18 Sector Owners and Operators' from the North
19 American Electric Reliability Corporation, acting in
20 its capacity as the Electricity Sector Information
21 and Analysis Center.
22 "(3) RESCISSION.—The Commission shall ap-
23 prove a reliability standard developed under section
24 215 that addresses a grid security vulnerability that
25 is the subject of a rule or order under paragraph (1)

1 or (2), unless the Commission determines that such
2 reliability standard does not adequately protect
3 against such vulnerability or otherwise does not sat-
4 isfy the requirements of section 215. Upon such ap-
5 proval, the Commission shall rescind the rule pro-
6 mulgated or order issued under paragraph (1) or (2)
7 addressing such vulnerability, effective upon the ef-
8 fective date of the newly approved reliability stand-
9 ard.

10 "(4) GEOMAGNETIC STORMS.—Not later than 1
11 year after the date of enactment of this section, the
12 Commission shall, after notice and an opportunity
13 for comment and after consultation with the Sec-
14 retary and other appropriate Federal agencies, issue
15 an order directing the Electric Reliability Organiza-
16 tion to submit to the Commission for approval under
17 section 215, not later than 1 year after the issuance
18 of such order, reliability standards adequate to pro-
19 tect the bulk-power system from any reasonably
20 foreseeable geomagnetic storm event. The Commis-
21 sion's order shall specify the nature and magnitude
22 of the reasonably foreseeable events against which
23 such standards must protect. Such standards shall
24 appropriately balance the risks to the bulk-power
25 system associated with such events, including any

1 regional variation in such risks, and the costs of
2 mitigating such risks.
3 "(5) LARGE TRANSFORMER AVAILABILITY.—
4 Not later than 1 year after the date of enactment
5 of this section, the Commission shall, after notice
6 and an opportunity for comment and after consulta-
7 tion with the Secretary and other appropriate Fed-
8 eral agencies, issue an order directing the Electric
9 Reliability Organization to submit to the Commis-
10 sion for approval under section 215, not later than
11 1 year after the issuance of such order, reliability
12 standards addressing availability of large trans-
13 formers. Such standards shall require entities that
14 own or operate large transformers to ensure, individ-
15 ually or jointly, adequate availability of large trans-
16 formers to promptly restore the reliable operation of
17 the bulk-power system in the event that any such
18 transformer is destroyed or disabled as a result of
19 a reasonably foreseeable physical or other attack or
20 geomagnetic storm event. The Commission's order
21 shall specify the nature and magnitude of the rea-
22 sonably foreseeable attacks or events that shall pro-
23 vide the basis for such standards. Such standards
24 shall—

1 "(A) provide entities subject to the stand-
2 ards with the option of meeting such standards
3 individually or jointly; and
4 "(B) appropriately balance the risks asso-
5 ciated with a reasonably foreseeable attack or
6 event, including any regional variation in such
7 risks, and the costs of ensuring adequate avail-
8 ability of spare transformers.
9 "(d) CRITICAL DEFENSE FACILITIES.—
10 "(1) DESIGNATION.—Not later than 180 days
11 after the date of enactment of this section, the
12 President shall designate, in a written directive or
13 determination provided to the Commission, facilities
14 located in the United States (including the terri-
15 tories) that are—
16 "(A) critical to the defense of the United
17 States; and
18 "(B) vulnerable to a disruption of the sup-
19 ply of electric energy provided to such facility
20 by an external provider.
21 The number of facilities designated by such directive
22 or determination shall not exceed 100. The Presi-
23 dent may periodically revise the list of designated fa-
24 cilities through a subsequent written directive or de-
25 termination provided to the Commission, provided

1 that the total number of designated facilities at any
2 time shall not exceed 100.
3 "(2) COMMISSION AUTHORITY.—If the Commis-
4 sion identifies a defense critical electric infrastruc-
5 ture vulnerability that the Commission, in consulta-
6 tion with owners and operators of any facility or fa-
7 cilities designated by the President pursuant to
8 paragraph (1), determines has not adequately been
9 addressed through measures undertaken by owners
10 or operators of defense critical electric infrastruc-
11 ture, the Commission shall, after notice and an op-
12 portunity for comment and after consultation with
13 the Secretary and other appropriate Federal agen-
14 cies, promulgate a rule or issue an order requiring
15 implementation, by any owner or operator of defense
16 critical electric infrastructure, of measures to protect
17 the defense critical electric infrastructure against
18 such vulnerability. The Commission shall exempt
19 from any such rule or order any specific defense
20 critical electric infrastructure that the Commission
21 determines already has been adequately protected
22 against the identified vulnerability. The Commission
23 shall make any such determination in consultation
24 with the owner or operator of the facility designated

1 by the President pursuant to paragraph (1) that re-
2 lies upon such defense critical electric infrastructure.
3 "(3) COST RECOVERY.—An owner or operator
4 of defense critical electric infrastructure shall be re-
5 quired to take measures under paragraph (2) only to
6 the extent that the owners or operators of a facility
7 or facilities designated by the President pursuant to
8 paragraph (1) that rely upon such infrastructure
9 agree to bear the full incremental costs of compli-
10 ance with a rule promulgated or order issued under
11 paragraph (2).
12 "(e) PROTECTION OF INFORMATION.—
13 "(1) PROHIBITION OF PUBLIC DISCLOSURE OF
14 PROTECTED INFORMATION.—Protected informa-
15 tion—
16 "(A) shall be exempt from disclosure under
17 section 552(b)(3) of title 5, United States Code;
18 and
19 "(B) shall not be made available pursuant
20 to any State, local, or tribal law requiring dis-
21 closure of information or records.
22 "(2) INFORMATION SHARING.—
23 "(A) IN GENERAL.—Consistent with the
24 Controlled Unclassified Information framework
25 established by the President, the Commission

1 shall promulgate such regulations and issue
2 such orders as necessary to designate protected
3 information and to prohibit the unauthorized
4 disclosure of such protected information.
5 "(B) SHARING OF PROTECTED INFORMA-
6 TION.—The regulations promulgated and orders
7 issued pursuant to subparagraph (A) shall pro-
8 vide standards for and facilitate the appropriate
9 sharing of protected information with, between,
10 and by Federal, State, local, and tribal authori-
11 ties, the Electric Reliability Organization, re-
12 gional entities, and owners, operators, and
13 users of the bulk-power system in the United
14 States and of defense critical electric infrastruc-
15 ture. In promulgating such regulations and
16 issuing such orders, the Commission shall take
17 account of the role of State commissions in re-
18 viewing the prudence and cost of investments
19 within their respective jurisdictions. The Com-
20 mission shall consult with appropriate Canadian
21 and Mexican authorities to develop protocols for
22 the sharing of protected information with, be-
23 tween, and by appropriate Canadian and Mexi-
24 can authorities and owners, operators, and

1 users of the bulk-power system outside the
2 United States.
3 "(3) SUBMISSION OF INFORMATION TO CON-
4 GRESS.—Nothing in this section shall permit or au-
5 thorize the withholding of information from Con-
6 gress, any committee or subcommittee thereof, or
7 the Comptroller General.
8 "(4) DISCLOSURE OF NON-PROTECTED INFOR-
9 MATION.—In implementing this section, the Com-
10 mission shall protect from disclosure only the min-
11 imum amount of information necessary to protect
12 the reliability of the bulk-power system and of de-
13 fense critical electric infrastructure. The Commission
14 shall segregate protected information within docu-
15 ments and electronic communications, wherever fea-
16 sible, to facilitate disclosure of information that is
17 not designated as protected information.
18 "(5) DURATION OF DESIGNATION.—Informa-
19 tion may not be designated as protected information
20 for longer than 5 years, unless specifically redesig-
21 nated by the Commission.
22 "(6) REMOVAL OF DESIGNATION.—The Com-
23 mission may remove the designation of protected in-
24 formation, in whole or in part, from a document or
25 electronic communication if the unauthorized disclo-

1 sure of such information could no longer be used to
2 impair the reliability of the bulk-power system or of
3 defense critical electric infrastructure.

4 "(7) JUDICIAL REVIEW OF DESIGNATIONS.—
5 Notwithstanding subsection (f) of this section or sec-
6 tion 313, a person or entity may seek judicial review
7 of a determination by the Commission concerning
8 the designation of protected information under this
9 subsection exclusively in the district court of the
10 United States in the district in which the complain-
11 ant resides, or has his principal place of business, or
12 in the District of Columbia. In such a case the court
13 shall determine the matter de novo, and may exam-
14 ine the contents of documents or electronic commu-
15 nications designated as protected information in
16 camera to determine whether such documents or any
17 part thereof were improperly designated as protected
18 information. The burden is on the Commission to
19 sustain its designation.

20 "(f) JUDICIAL REVIEW.—The Commission shall act
21 expeditiously to resolve all applications for rehearing of
22 orders issued pursuant to this section that are filed under
23 section 313(a). Any party seeking judicial review pursuant
24 to section 313 of an order issued under this section may

1 obtain such review only in the United States Court of Ap-
2 peals for the District of Columbia Circuit.
3 "(g) PROVISION OF ASSISTANCE TO INDUSTRY IN
4 MEETING GRID SECURITY PROTECTION NEEDS.—
5 "(1) EXPERTISE AND RESOURCES.—The Sec-
6 retary shall establish a program, in consultation with
7 other appropriate Federal agencies, to develop tech-
8 nical expertise in the protection of systems for the
9 generation, transmission, and distribution of electric
10 energy against geomagnetic storms or malicious acts
11 using electronic communications or electromagnetic
12 pulse that would pose a substantial risk of disrup-
13 tion to the operation of those electronic devices or
14 communications networks, including hardware, soft-
15 ware, and data, that are essential to the reliability
16 of such systems. Such program shall include the
17 identification and development of appropriate tech-
18 nical and electronic resources, including hardware,
19 software, and system equipment.
20 "(2) SHARING EXPERTISE.—As appropriate,
21 the Secretary shall offer to share technical expertise
22 developed under the program under paragraph (1),
23 through consultation and assistance, with owners,
24 operators, or users of systems for the generation,
25 transmission, or distribution of electric energy lo-

1 cated in the United States and with State commis-
2 sions. In offering such support, the Secretary shall
3 assign higher priority to systems serving facilities
4 designated by the President pursuant to subsection
5 (d)(1) and other critical-infrastructure facilities,
6 which the Secretary shall identify in consultation
7 with the Commission and other appropriate Federal
8 agencies.

9 "(3) SECURITY CLEARANCES AND COMMUNICA-
10 TION.—The Secretary shall facilitate and, to the ex-
11 tent practicable, expedite the acquisition of adequate
12 security clearances by key personnel of any entity
13 subject to the requirements of this section to enable
14 optimum communication with Federal agencies re-
15 garding grid security threats, grid security
16 vulnerabilities, and defense critical electric infra-
17 structure vulnerabilities. The Secretary, the Com-
18 mission, and other appropriate Federal agencies
19 shall, to the extent practicable and consistent with
20 their obligations to protect classified and protected
21 information, share timely actionable information re-
22 garding grid security threats, grid security
23 vulnerabilities, and defense critical electric infra-
24 structure vulnerabilities with appropriate key per-
25 sonnel of owners, operators, and users of the bulk-

1 power system and of defense critical electric infra-
2 structure.
3 "(h) CERTAIN FEDERAL ENTITIES.—For the 11-year
4 period commencing on the date of enactment of this sec-
5 tion, the Tennessee Valley Authority and the Bonneville
6 Power Administration shall be exempt from any require-
7 ment under subsection (b) or (c) (except for any require-
8 ment addressing a malicious act using electronic commu-
9 nication).".
10 (b) CONFORMING AMENDMENTS.—
11 (1) JURISDICTION.—Section 201(b)(2) of the
12 Federal Power Act (16 U.S.C. 824(b)(2)) is amend-
13 ed by inserting "215A," after "215," each place it
14 appears.
15 (2) PUBLIC UTILITY.—Section 201(e) of the
16 Federal Power Act (16 U.S.C. 824(e)) is amended
17 by inserting "215A," after "215,".
18 **SEC. 3. BUDGETARY COMPLIANCE.**
19 The budgetary effects of this Act, for the purpose of
20 complying with the Statutory Pay-As-You-Go Act of 2010,
21 shall be determined by reference to the latest statement
22 titled "Budgetary Effects of PAYGO Legislation" for this
23 Act, submitted for printing in the Congressional Record
24 by the Chairman of the House Budget Committee, pro-

1 vided that such statement has been submitted prior to the
2 vote on passage.

Mr. WHITFIELD. At this time I would like to yield for the purpose of an opening statement to Mr. Rush, the ranking member.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. I want to thank you, Mr. Chairman, thank you to all the distinguished guests for being here today.

Mr. Chairman, today we are holding a hearing on the Grid Reliability and Infrastructure Defense Act, or the GRID Act for short. This bipartisan piece of legislation is identical to the bill that was favorably reported out of the E&C Committee unanimously last year and then went on to pass the House by a voice vote before getting stalled in the Senate.

Mr. Chairman, this bill represents the type of legislation that advances the security interests of all Americans and shows what can be accomplished when we choose to work together in a bipartisan manner. So I appreciate you conducting this hearing today, Mr. Chairman, and I hope and expect that we will move this bill with the same type of cooperation and collaboration that we experienced last session as this legislation moves through the committee.

Mr. Chairman, the U.S. electric grid consists of interconnected transmission lines and local distribution systems that deliver electricity to our homes, schools, our offices, generation facilities and related communications systems. The intricate design of the grid makes all of our components highly interdependent so that problems in one location can lead to a domino effect of reliability concerns in other areas.

In today's highly digitized world, the operational controls over the transmission grid at generators are increasingly managed by computer systems such as the supervisory control and data acquisition, or SCADA systems, which are linked to the Internet or other communication systems as well as to each other. This reliance on automation and two-way communication amplifies the grid's vulnerability to remote cyber attacks. Additionally, the increased use of advanced metering systems and other smart grid capabilities leaves our electric grid even more open to attack.

Mr. Chairman, this bill will amend the Federal Power Act to add a new section, section 2015(a), which will give the Federal Energy Regulatory Commission, FERC, new authority to protect the electric grid from cyber attack as well as from other threats including those posed from geomagnetic storms created by solar activity.

Additionally, this bill will provide FERC with the authority to issue emergency orders to protect against a grid security threat whether by malicious act, a geomagnetic storm, or by targeted physical attacks if the President notifies the commission that such a threat exists.

Mr. Chairman, we are all aware of the constant potential threats that our Nation faces whether by countries such as China and Russia, who have already conducted cyber probes of the U.S. grid systems, or by terrorist organizations looking for ways to weaken our capabilities. Cyber attacks can cause untold harm to our Nation's grid, and they can be done from faraway locations at very, very low cost and with little ability to trace the source of these threats. So it is imperative that we provide those agencies that are responsible

for protecting us, protecting our Nation's grid, protecting all Americans with all the tools, all the authority and all the resources that they need to keep us safe.

So Mr. Chairman, I applaud you for holding this very important hearing today. I look forward to hearing from our witnesses and our experts on this critical issue, and with that, I yield back all the time that I have, which is 1 second.

Mr. WHITFIELD. Thank you for being so generous once again, Mr. Rush.

At this time I recognize the ranking member of the full committee, Mr. Waxman, for the purposes of an opening statement.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Mr. Chairman.

Today, the subcommittee examines the Grid Reliability and Infrastructure Defense Act. This legislation is as bipartisan as they come. This legislation was born out of a bipartisan realization that our electric grid simply isn't adequately protected from a range of potential threats. And the current process for addressing vulnerabilities in the electric grid is not sufficient.

In an emergency situation where the grid faces an imminent threat, the Federal Energy Regulatory Commission currently lacks authority to require the necessary protective measures. There are also an ever-growing number of grid security vulnerabilities. These are weaknesses in the grid that could be exploited by criminals, terrorists or other countries to damage our electric grid. These same weaknesses even make the grid vulnerable to naturally occurring geomagnetic storms.

During the last Congress, Chairman Upton, Representatives Ed Markey and Joe Barton and I developed the GRID Act on a bipartisan basis. The majority and minority staffs had extensive discussions with interested stakeholders and agencies. We worked with many members to answer their questions, address their concerns, and consider their constructive suggestions. This cooperative process produced strong bipartisan legislation.

On April 15, 2010, the committee favorably reported the bill by a unanimous vote of 47 to zero. And on June 9, 2010, the GRID Act passed the House by voice vote on the suspension calendar. Unfortunately, the GRID Act did not become law in the last Congress.

I commend the chairman for taking up the GRID Act for consideration in this Congress. This bipartisan legislation will provide the FERC with the authorities it needs to address imminent threats to the electric grid with temporary emergency orders. It also directs the Commission to address longer-term grid vulnerabilities with standards written or approved by the Commission.

In addition, the bill includes provisions that focus specifically on the portions of the grid that serve facilities critical to the defense of the United States. And the bill is budget neutral.

These are important national security and grid reliability issues. In the last Congress, we heard from the Defense Department and from former Defense Secretaries, National Security Advisors, and

CIA Directors. They all told us that the changes made by this bill are critical to our national security.

I look forward to hearing from today's witnesses. Although we are likely to hear some in industry argue against providing FERC authority to address these serious threats, we worked across the aisle in the last Congress to develop workable legislation. I hope today marks the beginning of a similar process in this Congress.

The GRID Act is simply too important to allow special interests to weaken its effectiveness. The Committee needs to act to protect the Nation's electric grid from cyber attacks, direct physical attacks, electromagnetic pulses and solar storms.

Thank you, Mr. Chairman.

Mr. WHITFIELD. Thank you.

OK. Today we have three panels of witnesses, and on the first panel, we have two Members of Congress, the Honorable Trent Franks of Arizona and Mr. Jim Langevin of Rhode Island. We appreciate both of you being here very much, and Mr. Franks, I will recognize you for a 5-minute opening statement.

STATEMENTS OF HON. TRENT FRANKS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARIZONA; AND HON. JAMES R. LANGEVIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF RHODE ISLAND

STATEMENT OF TRENT FRANKS

Mr. FRANKS. Well, thank you, Mr. Chairman, and good afternoon to you, sir, and to Ranking Members Rush and Waxman and the rest of the fellow members here on the committee.

I believe the subject of today's hearing is one of profound implication and importance to western civilization, and consequently, I hope the members will feel inclined to read my written testimony. I just thank you again for allowing me to testify here today.

Mr. Chairman, in our technological advancement, we have now captured the electron and transported its utility into nearly every business, home and industrial endeavor throughout the civilized world. In so doing, we have advanced our standard of living and productivity beyond dreams but we have also grown profoundly dependent upon electricity and its many accoutrements. In keeping with one of humanity's most reliable hallmarks, we now found among our greatest strengths an unsettling vulnerability to EMP, or electromagnetic pulse.

The effects of geomagnetic storms and electromagnetic pulses on electric infrastructure are well documented with nearly every space, weather and EMP expert recognizing the dramatic disruptions and cataclysmic collapses these pulses can bring to electric grids.

In 2008, the EMP Commission testified before the Armed Services Committee, of which I am a member, that the U.S. society and economy are so critically dependent upon the availability of electricity that a significant collapse of the grid precipitated by a major natural or manmade EMP event could result in catastrophic civilian casualties. This conclusion is echoed by separate reports recently compiled by the DO, DHS, DOE and the National Academy of Sciences along with various other government agencies and inde-

pendent researchers. All of them, Mr. Chairman, came to very similar conclusions. The sobering reality is that this vulnerability if left unaddressed could have grave societal-altering consequences.

Like many of you, I believe Federal regulations should be very limited. However, our first national priority is national security, and to protect our national security, we must protect our major transformers from cascading destruction. To that end, I have introduced the SHIELD Act, which differs primarily from your discussion draft in three critical areas. Unlike the GRID Act, which I commend this committee deeply for passing last year, the SHIELD Act authorizes to promulgate standards necessary to protect our electric infrastructure against both natural and manmade electromagnetic pulse events if the standards developed by the ERO are inadequate to protect national security. The SHIELD Act additionally requires automated hardware-based solutions rather than procedural and operational safety measures alone, and the SHIELD Act does not contain cybersecurity provisions, leaving the conflicting approaches to that extremely important issue among the Members of the Senate in particular to be debated in a separate bill.

Automated hardware, Mr. Chairman, is particularly important when one considers the shortcomings of procedural and operational safety measures alone in response to an EMP event. According to solar weather experts, there is only 20 to 30 minutes warning from the time we predict a solar storm that may affect us until the time it actually does. This is simply not enough time to implement procedures that will adequately protect the grid. Furthermore, these predictions are only accurate one out of three times. This places a crushing dilemma on industry, who must decide whether or not to heed the warning with the knowledge that a wrong decision either way could result in the loss of thousands or even millions of lives and massive legal ramifications beyond expression.

Mr. Chairman and members, we are now 65 years into the nuclear age, and the ominous intersection of jihadist terrorism and nuclear proliferation has been inexorably and relentlessly hurdling toward America and the free world for decades. But when we add the dimension of asymmetric electromagnetic pulses to the equation, we face a menace that may represent the gravest short-term threat to the peace and security of the human family in the world today. Certainly, there are those who believe that the likelihood of terrorists or rogue states obtaining nuclear weapons and using them in an EMP attack is remote and it may be a reasonable conclusion for the moment, but in the recent events of the Arab spring, which our intelligence apparatus did not foresee, it shows us that regimes can change very quickly. If terrorists or rogue states do acquire nuclear weapons, hardening our electric grid would immediately become a desperate national priority. However, that process will take several years, and a regime change only takes a few weeks, a missile launch only takes a few minutes. The fact that we are now 100 percent vulnerable means that we should start securing our electric infrastructure now. Indeed, by reducing our vulnerability, we may reduce the likelihood that terrorists or rogue states would attempt such an attack in the first place.

Thankfully, Mr. Chairman and members, there is a moment in the life of nearly every problem when it is big enough to be seen by responsible, reasonable people and still small enough to be solved. You and I live in that moment when there still may be time for the free world to address and mitigate the vulnerability that naturally occurring or weaponized EMP represents to the mechanisms of our civilization. Your actions today to protect America may gain you no fame or fanfare in the annals of history. However, it may happen that in your lifetime, a natural or manmade event so big has an effect so small that none but a few will recognize the disaster that was averted. And for the sake of our children and future generations, I pray it happens exactly that way.

Thank you, and God bless you all.

[The prepared statement of Mr. Franks follows:]

Testimony by Congressman Trent Franks to the Energy and Power Subcommittee

5-31-11

Good afternoon Chairman Whitfield, Chairman Upton, Ranking Members Rush and Waxman, and the rest of my fellow Members on the committee. I believe the subject of this hearing is one of profound implication and importance to Western civilization.

Thank you for allowing me to testify today.

In our technological advancement, we have now captured the electron and transported its utility into nearly every business, home and industrial endeavor throughout the civilized world. In so doing, we have advanced our standard of living and productivity beyond dreams. But we have also grown profoundly dependent upon electricity and its many accoutrements.
In keeping with one of humanity's most reliable hallmarks, we now find among our greatest strengths an unsettling vulnerability... EMP...Electromagnetic Pulse.

Catalyzed by a major solar storm, a high altitude nuclear blast, or a non-nuclear, device induced Intentional Electromagnetic Interference, this invisible force of ionized particles has the capability to overwhelm and destroy our present electrical power grids and electrical equipment, including electronic communication networks, radio equipment, integrated circuits and computers.

The effects of geomagnetic storms and electromagnetic pulses on electric infrastructure are well-documented, with nearly every space weather and EMP expert recognizing the dramatic disruptions and cataclysmic collapses these pulses can bring to electric grids. In 2008 the EMP Commission testified before The Armed Services Committee, of which I am a member, that the US society and economy are so critically dependent upon the availability of electricity that a significant collapse of the grid, precipitated by a major natural or man-made EMP event, could result in catastrophic civilian casualties. This conclusion is echoed by separate reports recently compiled by the DOD, DHS, DOE, NAS, along with various other government agencies and independent researchers. All came to very similar conclusions. The sobering reality is that this vulnerability, if left unaddressed, could have grave, societal altering consequences.

Like many of you, I believe Federal regulation should be very limited. Our first national security priority in this instance is to protect our major transformers from cascading destruction. To that end, I have introduced the SHIELD ACT, which differs primarily from your discussion draft in three critical areas. Unlike the GRID ACT, which I commend this committee for passing last year, the Shield Act authorizes FERC to promulgate standards necessary to protect our electric infrastructure against both natural and man-made electromagnetic pulse events if the standards developed by the ERO are inadequate to protect national security. THE SHIELD ACT additionally requires automated hardware-based solutions rather than procedural safety measures alone. And THE SHIELD ACT does not contain cyber security provisions, leaving the conflicting approaches to that extremely important issue, among members of the Senate in particular, to be debated in a separate bill.

Automated hardware is particularly important when one considers the shortcomings of procedural safety measures alone in response to an EMP event. According to solar weather experts, there is only 20-30 minutes warning from the time we predict a solar storm may affect us to the time it actually does. This is simply not enough time to implement procedures that will adequately protect the grid. Furthermore, these predictions are only accurate one out of three times. This places a crushing dilemma on industry, who must decide whether or not to heed the warning with the knowledge that a wrong decision either way could result in the loss of thousands or even millions of lives and massive legal ramifications beyond expression.

Mr. Chairman, the phenomenon of natural and man-made electromagnetic pulse is not a new one.

In 1859, English Astronomer Richard Carrington discovered the cause of natural EMP when he identified and chronicled a major geomagnetic solar storm which brilliantly intensified the Northern lights and caused the telegraph system, the only major electrical system that existed on earth at that time, to go down across the planet. The National Academy of Sciences predicts this effect, to a lesser or greater degree, will recur globally approximately once every 100 years.

In 1962, the United States discovered that a high altitude nuclear blast could generate a more localized electromagnetic pulse of the same intensity as the Carrington effect. In an upper atmospheric nuclear test called Starfish Prime, an EMP occurred and electric lines were fused and radios and street lights stopped working in Hawaii nearly 900 miles away. The residual effects also disabled nearly all major satellites systems.

Because of new understandings of how EMP interacts with the Earth's electromagnetic field, and that it is intensified over large land mass, we now believe that if a warhead with a nuclear yield of just 100 kilotons detonated at an altitude of 400 kilometers over America's heartland, the resulting damage to our electric grid and infrastructure would be catastrophic across most of the continental United States. Such a result would be devastating to our electricity, transportation, water and food supply, medical care, financial networks, telecommunication and broadcasting systems and our infrastructure in general. Under such a scenario, both military and productive capability would be devastated. The immediate and eventual impact, directly and indirectly, on the human population, especially in major cities, is unthinkable.

It should be remembered that EMP was first considered as a military weapon during the "Cold War" as a means of paralyzing U.S. retaliatory forces.

America's EMP commission began their 70 page executive summary describing a one or two missile EMP attack as one of the few threats which look as if it could defeat the US military.

Dr. William Graham, the chairman of the EMP Commission, testified before the U.S. House Armed Services Committee, and stated:

QUOTE "EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.

"...A determined adversary can achieve an EMP attack capability without having a high level of sophistication. For example, an adversary would not have to have long-range ballistic missiles to conduct an EMP attack against the United States. Such an attack could be launched from a

freighter off the U.S. coast using a short or medium range missile to loft a nuclear warhead to high altitude. Terrorists sponsored by a rogue state could potentially execute such an attack without revealing their identity." UNQUOTE

Dr. Graham has said that a major catastrophic EMP attack on the United States could cause an estimated 70-90 percent of the our nation's population to become unsustainable.

It is impossible for me to even wrap my mind around that figure.

But for terrorists, this is their ultimate goal, and I believe EMP is their ultimate asymmetric weapon. In 1988, Osama bin Laden called it a religious duty for al-Qaida to acquire nuclear weapons. U.S. Admiral Mike Mullen, the Chairman of the Joint Chiefs of Staff, has stated, QUOTE "My worst nightmare is terrorists with nuclear weapons. Not only do I know they are trying to get them, but I know they will use them." UNQUOTE

This is indeed the greatest danger of all. If a rogue state like Iran steps over the nuclear threshold, rogue regimes and terrorists the world over will have access to these monstrous weapons.

We do well to remember that Iran, the world's leading sponsor of international terrorism, has practiced launching a mobile ballistic missile from a vessel in the Caspian Sea. Iran has also tested high-altitude explosions of the Shahab-III, a test mode consistent with an EMP attack, and described the tests as successful. We have also discovered an Iranian military journal that included an article recommending such a strategy. The article noted that if major Western nations do not learn to defend themselves against EMP attacks, they will be destroyed.

On June 2nd of last year, Mahmoud Ahmadinejad again made it clear where he stands. Israel, he declared, "is about to die and will soon be erased from the geographical scene."

Jewish author, Primo Levi, was once asked what he had learned from the Holocaust. He replied, "When a man with a gun says he's going to kill you - believe him."

At this moment, Iranian President Mahmoud Ahmadinejad, a man who, in the same breath, both denies the Holocaust ever occurred, and then threatens to make it happen again, is arrogantly seeking a gun with which he vows to wipe the state of Israel off the map.

He has also said: "The time for the fall of the satanic power of the United States has come and the countdown to the annihilation of the emperor of power and wealth has started." He has said point-blank, "The wave of the Islamist revolution will soon reach the entire world."

What a happy cheerful, fellow…

Unfortunately, he talks like a man who knows something the rest of us don't.

It is not enough, to casually dismiss his fanatical rhetoric. When analyzing the nature of any threat, we must always seriously assess two things: a potential enemy's intent and his corresponding capacity to carry out any such intent.

Mahmoud Ahmadinejad and his regime have stated very clearly their intent to see Israel wiped off the face of the earth and America and the West brought to their knees. Nuclear warheads could give them the capacity to effectively proceed in that endeavor; and to ignore the incontrovertible fact that Iran is rapidly progressing toward a nuclear weapons capability, is to resign ourselves and our children to live and walk in the shadow of nuclear terrorism.

Mr. Chairman and Members, these things should not surprise us. We are now 65 years into the nuclear age, and the ominous intersection of jihadist terrorism and nuclear proliferation has been

inexorably and relentlessly rolling toward America and the free world for decades. But, when we add the dimension of asymmetric electromagnetic pulse attacks to that equation, we face a menace that may represent the gravest short term threat to the peace and security of the human family in the world today.

Certainly there are those who believe that the likelihood of terrorists or rogue states obtaining nuclear weapons and using them in an EMP attack is remote. It may be a reasonable conclusion for the moment. But the recent events of the Arab Spring, which our intelligence apparatus did not foresee, show us that regimes can change very quickly. Is a regime change in Pakistan possible? Will there be blowback from our involvement in Libya? What about the current crisis in Syria? Will North Korea ever supply or sell it nuclear technology or warheads to terrorists? Will Iran develop or obtain nuclear weapons?

If terrorists or rogue states do acquire nuclear weapons, hardening our electric grid would become a desperate priority for our nation. However, that process will take several years, while a regime change takes only weeks and a missile launch only minutes. The fact that we are now 100% vulnerable means we should start securing our electric infrastructure now. Indeed, by reducing our vulnerability we may reduce the likelihood that terrorists or rogue states would attempt such an attack.

We should always remember that seven decades ago, another murderous ideology arose in the world. The dark shadow of the Nazi swastika fell first upon the Jewish people of Germany. And because the world did not heed the warnings of men like Winston Churchill and respond to that

evil in time, it began to spread across Europe until it lit the fire's of World War II's hell on earth which saw atomic bombs fall upon cities and over 50 million people dead worldwide.

History has repeatedly shown humanity to be susceptible to malignant dangers that approach inaudibly and nestle among us with innocuous countenance until a day of sudden calamity finds us empty handed, broken hearted, and without excuse.

Thankfully, Mr. Chairman and Members, there is a moment in the life of nearly every problem when it is big enough to be seen by reasonable people and still small enough to be solved. You and I live in that moment when there still may be time for the free world to address and mitigate the vulnerability that naturally occurring or weaponized EMP represents to the mechanisms of our civilization.

The challenge to ultimately and fully protect our peoples and nations from all of the various perils of natural or manmade electromagnetic pulse will be long and lingering. But the time to protect our nation from the most devastating scenario is now; the threat is real, and the implications are sobering.

America's Brink Lindsey said it it this way, QUOTE "Here is the grim truth: We are only one act of madness away from a social cataclysm unlike anything our country has ever known. After a handful of such acts, who knows what kind of civilizational breakdown might be in store?"

Mr. Chairman and Members of the Committee, the first purpose of any government or its leaders is to protect the lives and security of its innocent citizens. The failure of this responsibility renders all others meaningless.

Your actions today to protect America may gain you no fame or fanfare in the annals of history. However, it may happen in your lifetime that a natural or man-made EMP event so big has an effect so small that no one but a few will recognize the disaster that was averted. For the sake of our children and future generations, I pray it happens exactly that way.

Thank you and God bless all of you.

IJN...

TRENT FRANKS
ARIZONA

JUDICIARY COMMITTEE
CHAIRMAN,
SUBCOMMITTEE ON THE CONSTITUTION

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON STRATEGIC FORCES

SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

Congress of the United States
Washington, DC

2435 RAYBURN BUILDING
WASHINGTON, DC 20515
(202) 225-4576

7121 W. BELL ROAD, SUITE 200
GLENDALE, AZ 85308
(623) 776-7911

www.house.gov/franks

June 6, 2011

The Honorable Ed Whitfield
Chairman
Subcommittee on Energy and Power
Energy and Commerce Committee
2125 Rayburn HOB
Washington, DC 20515

Dear Chairman Whitfield,

I ask that the following clarifying statement be included in the official record for the hearing that was held on Tuesday, May 31, 2011 entitled "Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act." Thank you for your consideration of this request.

"I was misinformed regarding a possible intrusion into Palo Verde Nuclear Plant's systems. But I do know that Palo Verde is improving cyber security protective measures consistent with evolving regulatory requirements and industry practices. This is a developing area and continued strengthening of cyber security methodology is an ongoing activity and a high priority for the industry."

Most sincerely,

Trent Franks
United States Congress

PRINTED ON RECYCLED PAPER

Mr. WHITFIELD. Thank you, Mr. Franks.

Mr. Langevin, you are recognized for a 5-minute opening statement.

STATEMENT OF JAMES R. LANGEVIN

Mr. LANGEVIN. I would like to thank you, Chairman Whitfield, and Ranking Member Rush and Ranking Member Waxman for allowing me to testify on what I believe to be one of the most critical national security issues facing our country today: securing our electric grid from cyber vulnerabilities, an issue to which I have devoted several years of my time and effort, and I wanted to be here with my colleague, Mr. Franks.

As both a member of the House Armed Services Committee as well as the House Permanent Select Committee on Intelligence, I sit at a very interesting nexus which gives me broad transparency into the national security challenges that face our Nation today, and I previously testified on this issue in 2009 after a bill that I drafted with then-Homeland Security Chairman Bennie Thompson, which was adapted into then-Chairman Markey's GRID Act, and I of course want to thank the committee for including me in this discussion again here today.

We know that there are a number of actors who seek to do harm to our networks from foreign nation-states, domestic criminals and hackers, to disgruntled employees, and as the threat and capability both grow, so does the risk to our critical infrastructure. Now, this threat is not new. In the 110th Congress as chairman of the Homeland Security Subcommittee with jurisdiction over cybersecurity, I conducted a detailed examination of cyber threats to our critical infrastructure, and I want to reiterate what I made clear in my previous testimony before this subcommittee. I believe we remain vulnerable to a cyber attack against the electric grid that could cause severe damage to our critical infrastructure, our economy, our security and even American lives.

Now, the vast majority of our critical assets are in private hands, and because fixing vulnerabilities can be costly, security can find itself in conflict with other priorities like profit, competition and accountability to shareholders. Sadly, the American people are the ones placed at risk when the owners of our critical infrastructure fail to prepare for the worst-case scenarios.

I was pleased by the early attention paid to the issue of cybersecurity by the Obama administration, and despite some delays in the process, I would like to commend the administration for taking some very serious steps in the right direction. Under the leadership of Cyber Coordination Howard Schmidt and his staff, the White House has released legislative guidance that envisions more government involvement in setting standards and best practices for cyber protection across all sectors of our critical infrastructure. This mirrors philosophically the framework of legislation I introduced earlier this year.

Now, DHS is also taking important steps to become more involved in securing our critical infrastructure. The establishment of the Industrial Controls Systems Computer Emergency Response Team, or ICS–CERT, under Sean McGurk, formalized a group of

experts and fly-away teams that could respond to cyber incidents across all sectors of our utilities.

However, a company must still request help from the government before it can be deployed, and the simple act of having to ask often forces decision makers and industry to steer clear of seeking help for these complex problems. I am pleased to see industry players increasingly stepping up to the plate to combat these threats but I fear they cannot most fast and far enough under the current system. As Michael Assante, the president of the National Board of Information Security Examiners and former chief security officer at the North American Electric Reliability Corporation, or NERC, testified last year, and I quote, "We are not only susceptible but we are not very well prepared."

Now, I supported the GRID Act as it moved through the House last year because it seems to address some of the unique political and regulatory challenges in our power industry today. Currently, we live under a system that does not prioritize security but actively penalizes open reporting and cooperation. The legislation that is before us today aims to correct this by allowing Federal regulators greater authority to protect Americans during times of imminent crisis. It also provides for the issuance of orders to identify and mitigate vulnerabilities to protect the bulk power system from cyber attacks. While this measure is a significant step forward, I would also encourage the committee to consider provisions in my legislation and in Senate and administration proposals that expand this model to other sectors of critical infrastructure and enhance the ongoing efforts of DHS to quickly respond to a major crisis.

I would also note my concern that by specifying only the bulk power system, this legislation excludes critical distribution systems that would leave major cities like New York and Washington unprotected by the broader provisions of this bill.

I will conclude by cautioning again that inaction on this issue will make our Nation increasingly vulnerable to cyber attacks from both outside and within. We know the threat exists, and we have an opportunity to address it before any further damage is caused. It is the responsibility of Congress and the administration to take the appropriate steps that will protect this Nation.

Once again, I would like to thank you, Chairman Whitfield and Ranking Member Rush as well as Ranking Member Waxman, for their attention to this very important issue and for the opportunity to testify here today. I certainly look forward to working with the Energy and Commerce Committee and to supporting your efforts to raise awareness about securing our critical infrastructure and protecting our citizens from cyber attack.

Thank you, and I yield back.

[The prepared statement of Mr. Langevin follows:]

Statement of James R. Langevin (RI-02)
Before the House Committee on Energy and Commerce,
Subcommittee on Energy and Power

Legislative Hearing on "Protecting the Electric Grid: H.R. ____,
the Grid Reliability and Infrastructure Defense Act"

May 31, 2011

I would like to thank Chairman Whitfield and Ranking Member Rush for allowing me to testify on what I believe to be one of the most critical national security issues facing our country: securing our electric grid from cyber vulnerabilities. The Committee has given much attention to this topic over the past several years, and I commend you and your staff for your work. I previously testified on this issue in 2009 after a bill I had drafted with then-Homeland Security Chairman Bennie Thompson was adapted into then-Chairman Markey's GRID Act, and I thank the committee for including me in this discussion again today.

Thirteen years ago, the President's Commission on Critical Infrastructure Protection released a report on the risks associated with interconnected computer systems on the bulk power system. The Commission stated 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."

In the years since, we have seen this prediction validated as cyber threats across the power sector persist, along with an inability of industry to fully address these vulnerabilities on their own. One of the more public unclassified examples was seen in August 2003, when a software malfunction known as a "race condition" was set up in the control systems of a major East Coast energy supplier. This bug stalled their alarm systems after three power lines went down simultaneously, ultimately leading to a cascade failure of the entire Northeast power grid. The outage affected 55 million US and Canadian citizens and caused interruptions to water supplies, transportation systems, and cellular communications.

Unfortunately, cyber incidents on control systems aren't limited to accidents. Press reports have detailed the shocking threats that our increasingly networked critical infrastructure could pose to our electrical grid.

The Wall Street Journal in 2009 reported that foreign adversaries had penetrated and mapped our electrical grid, potentially leaving behind software that could disrupt our systems. Another major cyber incident, the STUXNET worm, has more recently demonstrated that online actors are aware of the cyber vulnerabilities of critical infrastructure, and are able to design weapons to exploit them. Noting the fear that such a weapon could one day be leveled against American critical infrastructure, the acting director of DHS's Cybersecurity Center noted that STUXNET "significantly changed the landscape of targeted cyberattacks."

We know that there are a number of actors who seek to do harm to our networks -- from foreign nation states, to domestic criminals and hackers, to disgruntled employees. And as threats and capability grow, so does the risk of a cyber attack on our critical infrastructure.

This threat is not new. In 2009, I testified before this Subcommittee about the threats to our bulk power system from cyber attack, and I want to reiterate what I made clear in my previous testimony: I believe we remain vulnerable to a cyber attack against the electric grid that could cause severe damage to our critical infrastructure, our economy, our security and even American lives.

Federal agencies have taken steps to reduce these vulnerabilities, but I am afraid that many in industry – and some in government -- still fail to appreciate the urgency of this threat. Since I began working on this issue, I have been disappointed by the overall lack of a serious response and commitment from the private sector. I held a hearing in 2007 examining the threats from an "Aurora"-like attack on our national power grid. At that time industry representatives lied to my Committee about having the situation fully under control. We caught them and they retracted their statements, but this attitude shows how difficult it can be to require and ensure security when it comes to critical infrastructure.

The vast majority of our critical assets are in private hands. In many sectors, private entities are largely self-regulated and are responsible for developing and implementing their own standards according to their own priorities. Because fixing vulnerabilities can be costly, security can find itself in conflict with other priorities like profit, competition, and accountability to shareholders. Sadly, the American people are the ones placed at risk when the owners of our critical infrastructure fail to prepare for worst-case scenarios.

I was pleased by the early attention paid to the issue of cybersecurity by the Obama Administration. In 2008, I worked with the transition team to highlight some cyber priorities from a congressional perspective, and it was clear even then that the incoming Administration understood the significance of the threat and planned to focus on the issue. Very soon after taking office, President Obama moved forward with the 60-day cyber review, becoming the first major world leader to take such action.

While progress has been slow at times, I would like to commend the Administration for taking some very serious steps in the right direction. Under the leadership of Cyber Coordinator Howard Schmidt and his staff, the White House has now released legislative guidance in response to much of the work already being done in Congress on this issue. Their recommendations envision more government involvement in setting standards and best practices for cyber protection across all sectors of our critical infrastructure, and mirror the philosophical framework of legislation I introduced earlier this year.

DHS has also taken important steps to become more involved in securing our critical infrastructure. The establishment of the Industrial Control Systems Computer Emergency Response Team, or ICS-CERT, under Sean McGurk, formalized a group of experts and fly-away teams that could respond to cyber incidents across all sectors of our utilities. However, a utility must first request help from the government before these resources can be brought to bear.

Unfortunately, the simple act of having to ask often forces decision makers in industry to steer clear of any government involvement for fear of embarrassment or competitive disadvantage. This leaves many owners and operators left to build piecemeal responses to what are often larger and highly sophisticated cyber problems.

I am pleased to see industry players increasingly stepping up to the plate to combat these threats, but I fear they cannot move fast or far enough under the current system. In discussing industry's current readiness to meet these new threats, Michael Assante, the president of the National Board of Information Security Examiners and former Chief Security Officer at the North American Electric Reliability Corporation (NERC) said, "We're not only susceptible, but we're not very well prepared." Threats like STUXNET have been a wake-up call, and the time is right for government to work with industry partners to address the shortfalls in our current regulatory regime.

I supported the GRID Act as it moved through the House last year, because it seeks to address some of the unique regulatory challenges in our power industry today. Currently we live under a system that does not prioritize security, but actively penalizes open reporting and cooperation. The legislation aims to correct this by allowing Federal regulators greater authority to protect Americans during times of imminent crisis. It also provides for the issuance of orders to identify and mitigate vulnerabilities to protect the bulk power system and defense critical electric infrastructure (DCEI) from cyber attacks, direct physical attacks, manmade EMP, and geomagnetic storms.

While this measure is a significant step forward, I would also strongly encourage the Committee to consider provisions in my legislation, and in Senate and Administration proposals, that expand this model to other sectors of critical infrastructure and enhance the ongoing efforts of DHS to quickly respond to a major crisis. I would also note my concern that by specifying only the "bulk power system," this legislation excludes critical distribution systems that would leave major cities, like New York and Washington, D.C., unprotected by the broader provisions in the bill.

I'll conclude by cautioning again that inaction on this issue will make our nation increasingly vulnerable to cyber attacks, from both outside and within. We know the threat exists and we have an opportunity to address it before any further damage is caused. It is the responsibility of Congress and the Administration to take the appropriate steps that will protect this nation.

I want to once again thank Chairman Whitfield and Ranking Member Rush for their attention to this important issue and for the opportunity to testify. I look forward to working with the Energy and Commerce Committee and to supporting your efforts to raise awareness about securing our critical infrastructure and protecting our citizens from cyber attack. Thank you.

Mr. WHITFIELD. Thank you, Mr. Langevin. We appreciate the testimony of both of you.

As you know, this is an important issue with great consequences for the country, and last year, of course, the GRID Act did pass the House of Representatives but was unable to get through the Senate, and we are quite familiar with that. We pass a lot of things here that don't get through the Senate, but our objective is to get something through the House and the Senate and signed by the President. And I know, Mr. Franks, that a large number of members of the Armed Services Committee, and you serve on that as well, Mr. Langevin, are cosponsoring your bill, and I am assuming, Mr. Langevin that your bill and Senator Rockefeller's bill basically reflects the administration's proposal. Is that correct?

Mr. LANGEVIN. Well, I wouldn't go so far as to say that, but they both move in a similar direction.

Mr. WHITFIELD. What I would like from both of you to just give advice to this committee on what you think we need to do to maximize our opportunity to get this passed in the Senate. Mr. Franks?

Mr. FRANKS. Well, Mr. Chairman, as it happened last year, I went over and personally lobbied the Senate as hard as I could on the GRID Act, even though as I have laid out today, I believe that there are some critically important things that needed to be added to or changed. I met with Senator Murkowski and others there in the chamber, and the big challenge was that they had differing strategies on what should be done about cybersecurity.

Now, let me make it so desperately clear here. I believe that cybersecurity is a critically important issue, and I think I would find myself largely in Mr. Langevin's camp on that issue, but the problem is, the personalities there have different strategies on how to address it, and I am trying to protocol here, Mr. Chairman. They couldn't get together on that, and that is why we felt like the issue should be separated, not because that one is more important than the other per se but because I just think it is going to be especially difficult. That is complicated this year, as you know. The White House just a few weeks ago, probably what you were talking about with Mr. Langevin, released a legislative proposal for nationwide cross-sector cybersecurity efforts, and the Senate is working to produce a goal to meet those needs, and my concern is that if we tie them together, we may weaken both of them, because there is very little disagreement on the EMP aspects of it. The Senators were very supportive of being able to protect the grid itself, just had some very seriously differing approaches to the cybersecurity element of it.

Mr. WHITFIELD. OK. Mr. Langevin, do you have a comment?

Mr. LANGEVIN. Well, Mr. Chairman, I would just say that last year we were a bit frustrated by the Senate still contemplating which path forward they were going to take. I was fortunate to get an amendment included in the House Armed Services defense authorization bill last year that would have established a White House Office on Cybersecurity with a director's position that would have been Senate confirmed, and it would have included updates to the FISMA law. That did not get through the conference committee last year because the Senate was still struggling to determine which direction they were going to take, whether it was going

to be Rockefeller-Snowe or Collins-Lieberman. I believe that the Senate is moving in the direction of resolving those issues, and I am hopeful that now that the White House has come out with its guidance on their views on cybersecurity going forward that that will clear some of the hurdles in the Senate and they will be able to come together and reach an agreement which hopefully will allow the GRID Act, will allow these issues to clear the hurdles that remain ahead.

So I would say it is perseverance. We are going to have to continue to keep the pressure on the Senate but hopefully, and I would say that I am I close contact with Senator Sheldon Whitehouse, who is also from Rhode Island and who is also one of the leaders in the Senate on cybersecurity. He believes that we will see quite positive progress on the issue of cybersecurity in the Senate, so I am hopeful that we will see a lot of these issues addressed and we will be able to get them through conference.

Mr. WHITFIELD. Well, thank you all very much, and we do look forward to continuing to work with you because both of you have been leaders in this area and we hope that we can continue to call on you for your input.

At this time I will recognize the gentleman from Illinois.

Mr. RUSH. Thank you, Mr. Chairman. I am going to be brief.

Mr. Langevin, you have expressed some level of restraint regarding this bill in that you think that it could be strengthened in certain areas, and I am curious, I know that we want to send the best bill that we can to the Senate. Again, we can persevere, as you have indicated, but how do you think that we can strengthen this bill?

Mr. LANGEVIN. Well, a couple of things, Congressman Rush. I would like to see the approach that we are taking here, addressing the challenges to the bulk power system broadened to include other areas of critical infrastructure, because some of them would be in the jurisdiction of the full Energy and Commerce Committee. Others may be in the area of the Financial Services Committee. But I think that the approach that you are taking here is a positive one with respect to the electric grid.

In addition to that, I would like to see this bill address distribution systems, not just transmission but distribution systems. As I said, it is my understanding that because distribution is not dealt with in the bill that areas like Washington, D.C., and New York would be left out of the intent and hopefully the coverage that this legislation would provide, protection provided to our electric grid. So I would encourage the committee to look further at that issue.

Mr. RUSH. Congressman Franks, do you have any suggestions along the same lines?

Mr. FRANKS. Well, I think that Congressman Langevin has it absolutely right, that I know we have pictures of New York and Washington but we still want to keep them around for a while, and I think that it is wise to extend that to the transmission lines.

Again, my primary purpose here is to try to focus as narrowly as I can on maintaining the base electric grid, because if that goes down, our cybersecurity issues are no longer an issue because we don't have computer systems, we don't have the electricity to run them, and it might behoove the committee to consider a possibility

of sending the GRID Act over as it is and in a separate version just addressing the EMP issue in case there is the issue where the Senate can't come together on exactly how they want to do the cybersecurity, but I emphasize one last time that the cybersecurity issue is absolutely critical. I visited the Palo Verde nuclear power plant in Arizona just outside by district. It is the largest one in the Nation. And we had a hacker that was strokes away from being able to go in and begin to monkey with the reactor itself.

Mr. RUSH. Mr. Chairman, my general assembly and my State legislature, they just yesterday passed a bill out and sent it to the governor addressing some of these same matters, and I am interested in the other cities that you named but I am also interested in the third city, the city by the lake, Chicago, and what the threats are to Chicago also.

So with that, Mr. Chairman, I yield back the balance of my time.

Mr. WHITFIELD. Thank you, Mr. Rush.

Generally speaking, when we have Members of the House or the Senate testifying, the chairman and ranking member are the only ones that ask questions. However, I would ask our friends on this side of the aisle if they have any questions. Mr. Terry?

Mr. TERRY. I don't, but I have worked with Trent on his bill and I just wanted to thank both of you for your good work. This is an extremely important issue, and as the ranking member and the chairman both said, we need to get this to the point where the Senate can pass it and we get it to the President's desk, so thank you for your efforts. I yield back.

Mr. WHITFIELD. Well, thank you, Mr. Terry, and once again, thank you all so much for your concern and your leadership on this issue, and we will continue to work with you as we move forward, and unless you all want to stay and hear the other panel, we will let you go on in your other activities. So thank you.

Mr. LANGEVIN. Thank you.

Mr. FRANKS. Thank you, Mr. Chairman.

Mr. WHITFIELD. At this time I would like to call up our second panel, which includes the Honorable Patricia Hoffman, who is the Assistant Secretary, Office of Electricity Delivery and Energy Reliability at the Department of Energy. We have the Honorable Paul Stockton, Assistant Secretary of Defense for Homeland Security and America's Security Affairs at the U.S. Department of Defense, and we have Mr. Joseph McClelland, who is the director of the Office of Electric Reliability at FERC.

So welcome to the hearing, and thank you all for taking time to be with us and to give us your expertise and thoughts on this issue. So at this time, Ms. Hoffman, I will recognize you for a 5-minute opening statement, and I would just point out there is a little device on the top of the table that has a red, green and yellow light, and when it turns red, we would like for you to maybe think about coming to an end, but we won't hold strictly to that.

Ms. Hoffman, you are recognized for 5 minutes.

STATEMENTS OF PATRICIA A. HOFFMAN, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY; PAUL N. STOCKTON, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND AMERICAS' SECURITY AFFAIRS, DEPARTMENT OF DEFENSE; AND JOSEPH H. MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

STATEMENT OF PATRICIA A. HOFFMAN

Ms. HOFFMAN. Good afternoon, Mr. Chairman and members of the committee. I would like to extend my thanks to the chairman and the esteemed members of the committee for inviting me here today to discuss cybersecurity issues facing the electric industry, as well as potential legislation intended to strengthen protection of the bulk power system and the electric infrastructure.

Ensuring a resilient electric grid is particularly important, since it is arguably the most complex and critical infrastructure that others depend upon to delivery essential services. The Department of Energy's Office of Electricity Delivery and Energy Reliability supports the administration's strategic, comprehensive approach to cybersecurity, and specifically with respect to the electric grid, we recognize that our focus should be on seven key areas. One is facilitating public-private partnerships to accelerate grid cybersecurity efforts; two, funding research and development of advanced technology to create secure and resilient electricity infrastructure; three, developing cybersecurity standards that provide a baseline to protect against known vulnerabilities; four, timely sharing of information; five, the development of risk management frameworks; six, facilitation of incident management and response capabilities; and seven, the development of a highly skilled and adaptive workforce.

Cybersecurity for the electric grid must not only address threats and vulnerabilities of traditional information systems but also address the unique issues to electric control systems such as SCADA systems and other control devices.

The Cyberspace Policy Review underscores the need to strengthen public-private partnerships in order to design a more secure technology and improve resilience of the critical government and industry systems and networks. As directed by HSPD–7, a public-private partnerships must be established to effectively address national security concerns for critical infrastructure. However, private industry alone cannot be responsible for preventing, deterring, and mitigating effects of deliberate efforts to destroy or exploit critical infrastructure systems. Our Office has long recognized that neither the government nor the private sector nor individual citizens can meet cybersecurity challenges alone. We must work together.

OE supports and funds activities to enhance cybersecurity in the energy sector. Nearly all of the cybersecurity activities involve public and private partnerships. Through partnerships and competitive solicitations with the DOE, Department of Energy National Laboratories, industry and academia, OE has sponsored research and development of several advanced cybersecurity technologies that are commercially available, and a couple of these examples include a secure serial communications for control system that has been

commercialized by Sweitzer Engineering Laboratory; a software toolkit that provides auditing of SCADA security settings—this was commercialized by Digital Bond, which is a small business; vulnerability assessments of 38 different SCADA systems; and a common vulnerabilities report to help utilities and vendors mitigate vulnerabilities found in many SCADA systems.

Supporting the development of cybersecurity standards—our office is collaborating with NIST and other agencies and organizations to develop a framework and roadmap for interoperability standards that include cybersecurity as a critical element. The NIST smart grid interoperability panel cybersecurity working group released the Cybersecurity Guidelines for the Smart Grid. OE also partnered with leading utilities to develop cybersecurity profiles to provide vendor-neutral actionable guidance to utilities, vendors and government entities on building cybersecurity into the smart grid components at the development stage including safeguards and implementing safeguards when integrated into the grid.

OE supports continued investment in developing and building a cybersecurity workforce within the energy sector. Some examples include working with State and local governments and agencies to put together technical briefs, education forums, workshops and exercises, just to name a few.

The Department fully supports the administration's proposed comprehensive cybersecurity legislation focused on cybersecurity for the American people, our Nation's critical infrastructure and the Federal Government's own networks and computers. Specifically, the administration proposes the following legislative changes to enhance protection of critical infrastructure: voluntary government assistance to industry, voluntary sharing with industry and States and critical infrastructure security risk mitigation.

In conclusion, I would like to thank the committee for its leadership and supporting the protection of the bulk power system and critical infrastructure against cyber threats. The OE looks forward to working with Congress to further the dialog, and I would be pleased to answer any questions that you may have.

[The prepared statement of Ms. Hoffman follows:]

STATEMENT OF

PATRICIA HOFFMAN

ASSISTANT SECRETARY

OFFICE OF

ELECTRICITY DELIVERY AND ENERGY RELIABILITY

U.S. DEPARTMENT OF ENERGY

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON ENERGY AND POWER

UNITED STATES HOUSE OF REPRESENTATIVES

May 31, 2011

Chairman Whitfield, Ranking Member Rush and members of the Subcommittee, thank you for this opportunity to discuss the cyber security issues facing the electric industry, as well as potential legislation intended to strengthen protection of the bulk power system and electric infrastructure from cyber security threats.

Title XIII of the Energy Independence and Security Act of 2007 (EISA) states, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure." The protection and resilience of critical national infrastructures is a shared responsibility of the private sector, government, communities, and individuals. As the complexity, scale, and interconnectedness of today's infrastructures have increased, it has changed the way services and products are delivered, as well as the traditional roles of owners, operators, regulators, vendors, and customers.

Ensuring a resilient electric grid is particularly important since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services. Over the past two decades, the roles of electricity sector stakeholders have shifted: generation, transmission, and delivery functions have been separated into distinct markets; customers have become generators using distributed generation technologies; and vendors have assumed new responsibilities to provide advanced technologies and improve security. These changes have created new responsibilities for all stakeholders in ensuring the continued security and resilience of the electric power grid.

The Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) supports the Administration's strategic comprehensive approach to cyber security, focusing on the following key areas: public-private partnerships to accelerate smart grid cyber security efforts; research and development of advanced technology to create a secure and resilient electricity infrastructure; cyber security standards to provide a baseline to protect against known vulnerabilities; facilitating timely sharing of relevant and actionable threat information; risk management frameworks with private sector risk management plans subject to performance evaluation; incident management and response; and development of a highly skilled and adaptive workforce.

Cyber security Activities and Accomplishments

For more than a decade, the OE has been substantively engaged with the private sector to secure the electric grid. In December 2003, the Homeland Security Presidential Directive 7 (HSPD-7) designated the Department as the sector-specific agency (SSA) for the energy sector responsible for collaborating with all federal agencies, state and local governments, and the private sector. As the SSA, OE, representing the Department, works closely with the private sector and state/Federal regulators to provide secure sharing of threat information, to collaborate with industry to identify and fund gaps in infrastructure research, development and testing efforts, to conduct vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

The 2010 *National Security Strategy* underscores the need to strengthen public-private partnerships in order to design more secure technology that will better protect and improve the resilience of critical government and industry systems and networks. OE has long recognized that neither government, nor the private sector, nor individual citizens can meet cyber security challenges alone. In 2006, OE facilitated the development of the *Roadmap to Secure Control Systems in the Energy Sector* to provide a detailed collaborative plan for improving cyber security in the energy sector and concrete steps to secure control systems used in the electricity and oil and natural gas sectors. The plan calls for a 10-year implementation timeline with a 5-year update scheduled for release in the summer of 2011. To implement the priorities in the *Roadmap*, the Energy Sector Control Systems Working Group was formed and comprised of cyber security and control systems experts from government, the electricity sector, and the oil and natural gas sector.

Since 2006, the *Roadmap* has provided a collaborative strategy for prioritizing cyber security needs and focusing actions under way throughout government and the private sector to ensure future energy system security. The *Roadmap* goals and strategy have also been fully integrated into the *Energy Sector-Specific Plan*. Since the *Roadmap* was released, important progress has been made in improving cyber security in the energy sector. These improvements have benefited existing systems and are contributing to the secure design and integration of advanced systems that incorporate smart grid technologies.

Through competitive solicitations and partnerships with industry, academia and national laboratories, OE has supported the development of several advanced cyber security technologies that are now commercially available within the energy sector:

- A technology to secure serial communications for control systems, based on the Secure Supervisory Control and Data Acquisition (SCADA) Communications Protocol developed by the Pacific Northwest National Laboratory. This technology is rapidly being adopted by utilities.

- Software toolkits, available for download from the vendor website, that let electric utilities audit the security settings of SCADA systems. The latest release addresses the Inter-Control Center Communications Protocol (ICCP), which is used for utility-to-utility communications.

- Monitoring modules that aggregate security events from a variety of data sources on the control system network and then correlate the security events to help utilities better detect cyber attacks.

- An Ethernet security gateway, based on an interoperable design developed by Sandia National Laboratories, that secures site-to-site Ethernet communications and protects private networks.

OE established the National SCADA Test Bed in 2003 to provide a national capability for cyber security experts to systematically evaluate the components of a functioning system for inherent vulnerabilities, develop mitigations, and test the effectiveness of various cyber security technologies. Major accomplishments include:

- Completed vulnerability assessments of 38 SCADA systems and provided mitigation recommendations. As a result, vendors have implemented many of the recommendations in "hardened" next-generation SCADA systems that are now commercially available and being deployed in the power grid.

- Utility groups have also formed partnerships to fund additional cyber security assessments at the test bed to address specific cyber security concerns.

- Provided advanced cyber security training for over 2300 representatives from over 200 utilities to demonstrate how to detect and respond to complex cyber attacks on SCADA systems.

- Developed the "Common Cyber Security Vulnerabilities Observed in Control System Assessments" report to help utilities and vendors mitigate vulnerabilities found in many SCADA systems. OE has also worked with the North American Electric Reliability Corporation (NERC) to develop the *Top Ten Vulnerabilities of Control Systems and their Associated Mitigations* report in 2006 and 2007.

OE is also working closely with academic and industry partners through the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), which is a University led public-private research partnership supported by OE, Department of Homeland Security (DHS), and Industry for frontier research that supports resilient and secure smart grid systems. TCIPG leverages and expands upon previous research funded primarily by the National Science Foundation. TCIPG research focuses on building trusted energy delivery control systems from un-trusted components, and transitioning next-generation cyber security technologies to the energy sector. As an example, TCIPG released the Network Access Policy Tool that is now being used by industry and asset owners to characterize the global effects of local firewall rules in control system architectures. The tool will help utilities better manage and maintain security on their highly-complex communications networks.

Just recently, OE launched several new initiatives to enhance cyber security in the energy sector.

- OE, in coordination with DHS and other Federal agencies, has conducted several cyber threat information sharing workshops to analyze classified information, determine the impact to the sector, and develop mitigations that were specifically designed to work in the sector. This cooperative process has proven to be more effective and accepted than dictating solutions to the sector.

- OE, working with the National Institute of Standards and Technology (NIST), DHS, the Federal Energy Regulatory Commission (FERC), and NERC, is leading a collaborative effort with representatives from across the public and private sectors to develop a cyber security risk management guideline. The objective of this effort is to provide a consistent, repeatable, and adaptable process for the electric sector, and enable organizations to proactively manage risk.

Ensuring the cyber security of a modern, digital electricity infrastructure is a key objective of national smart grid efforts. As a result, a number of key initiatives have been developed to ensure future system security and enable the energy sector to better design, build, and integrate smart grid technologies. OE has engaged in partnerships to perform these activities with key organizations including FERC, the U.S. Department of Commerce, NIST, DHS, the Federal Communications Commission, the Department of Defense (DoD), the intelligence community, the White House Office of Science and Technology Policy, state public utility commissions, the National Association of Regulatory Utility Commissioners, NERC, the Open Smart Grid Subcommittee, Electric Power Research Institute (EPRI), and other energy sector organizations.

The American Recovery and Reinvestment Act of 2009 accelerated the development of smart grid technologies by investing in pilot projects, worker training, and large scale deployments. This public-private investment worth over $9.6 billion was dedicated to a nationwide plan to modernize the electric power grid, enhance the security of U.S. energy infrastructure, and promote reliable electricity delivery. The $4.5 billion in Recovery Act funds, managed by OE, was leveraged by $5.1 billion in funds from the private sector to support 132 Smart Grid Investment Grant and Smart Grid Demonstration Grant projects across the country. Each project awardee committed to implementing a cyber security plan that includes an evaluation of cyber risks and planned mitigations, cyber security criteria for device and vendor selection, and relevant standards or best practices the project will follow.

As called for in Section 1305 of EISA, OE is collaborating with NIST and other agencies and organizations to develop a framework and roadmap for interoperability standards that includes cyber security as a critical element. As part of this effort, NIST established the public-private Smart Grid Interoperability Panel, and within that, the 450-member Cyber Security Working Group (CSWG) to lead the development of cyber security requirements for the smart grid. After engaging members in numerous workshops and teleconferences and following two formal reviews, the CSWG released the first version of its *Guidelines for Smart Grid Cyber Security*. The three-volume document details a strategy that includes smart grid use cases, a high-level smart grid risk assessment process, smart grid-specific security requirements, development of a security architecture, assessment of smart grid standards, and development of a conformity assessment program for requirements.

To address cyber security needs for smart grid technologies, OE partnered with leading utilities and EPRI to develop cyber security profiles for major smart grid applications – Advanced Metering Infrastructure, Third-Party Data Access, and Distribution Automation. These profiles provide vendor-neutral, actionable guidance to utilities, vendors and government entities on how to build cyber security into smart grid components in the development stage, and how to implement those safeguards when the components are integrated into the power grid. These documents support the NIST "Cyber Security Guidelines for the Smart Grid" NISTIR – 7628. OE also co-chairs the NIST CSWG.

DOE Comments on Proposed Legislation

The Administration has proposed comprehensive cyber security legislation which was transmitted to May 12, 2011, (http://www.whitehouse.gov/omb/legislative_letters) focused on improving cyber security for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers. Specifically, the Administration proposes the following changes to current law to enhance protection of critical infrastructure:

1) Voluntary government assistance to industry, states, and local government to improve the Government's (DHS and sector specific agencies) ability to provide technical support, share cyber security information and expertise available to state and local governments and the private sector on request and on a voluntary basis with appropriate legal, privacy, and civil liberties safeguards.
2) Voluntary information sharing with industry, states, and local government to remove barriers that hinder voluntary sharing of cyber security information between the government and industry for cyber security purposes, and help improve overall situational awareness of threats and vulnerabilities in cyberspace.
3) Critical infrastructure cyber security risk mitigation to create a flexible framework for enhanced cooperation between the Government and critical infrastructure operators nationwide.

The Administration looks forward to working with Congress to enact these legislative changes..

We also understand that the Committee is currently considering reintroduction of "The Grid Reliability and Infrastructure Defense Act" (GRID Act). The Administration has no formal position on this legislation, and as noted above, we have a proposal of our own that we believe provides the best and most effective course of action. At the Committee's request, we are providing the following observations on existing authorities.

Processes for the development of risk frameworks, risk management plans, and implementation of performance evaluations for electric grid cyber security should be consistent with the Administration's cyber security legislation proposal. The Administration's proposal seeks to improve cyber security across the range of critical infrastructure sectors, while also recognizing the unique requirements for resilience and reliability and the important roles, responsibilities, and resources of the government and private sector entities within the electric sector.

Conclusion

In conclusion, I would like to again thank this Subcommittee for its leadership in supporting the protection of the bulk power system and critical electric infrastructure against cyber security threats. Recognizing the interdependencies between different sectors, it is important to have a comprehensive, government-wide strategy for cyber security legislation. DOE looks forward to working with Congress to enact comprehensive cyber security legislation that will enhance the protection of critical infrastructure as specified in the Administration's bill.

I would be pleased to address any questions the Subcommittee might have.

Mr. WHITFIELD. Thank you, Ms. Hoffman.

Mr. Stockton, you are recognized for 5 minutes.

STATEMENT OF PAUL N. STOCKTON

Mr. STOCKTON. Thank you, Mr. Chairman, Mr. Ranking Member and other distinguished members of the committee. I have a detailed statement which I will submit for the record, but I want to focus on a few key points that I make that I hope will be helpful to you as you exercise the leadership that we need coming from the House of Representatives and the Congress as a whole.

First of all, the Department of Defense is not in the lead for energy security in the United States. For the Federal Government, that is my colleagues at the Department of Energy, Department of Homeland Security, Department of Defense in support of them but let me emphasize, the Department of Defense cannot execute its core missions in service of this Nation unless we have a secure flow of commercial electric power, and that is for a simple reason: the Department of Defense depends for its energy 99 percent on the commercial sector. We don't own the commercial sector. We never will. We have no regulatory authority over it, but we are utterly dependent on the flow of that commercial power.

Let me talk a little bit about why that is the case. In the modern way of warfare, since 9/11, our forces deployed abroad fighting in Afghanistan and Iraq and operating elsewhere depend to an increasing extent on military facilities back here in the United States to conduct and support those operations. To generate, deploy and operate forces abroad, we depend on military facilities in the States represented here today, and if there is an interruption in the flow of commercial power to those facilities, for a short period they have backup power generation but for a longer disruption of the grid we would be facing a situation of potentially devastating effects on our conduct of defense operations abroad, and we could face serious challenges at home. I will talk about those consequences in a moment, but first I want to talk a little bit about the nature of the threat.

First of all, the cyber threat is something we take very, very seriously. That is why I am so strongly in support of the administration's cybersecurity legislative proposal. But I want to emphasize that cyber is only one of the threat vectors that the Nation faces. Simple kinetic attacks intelligently conducted by the adversary could have significant disruptive effects on the flow of commercial power to Department of Defense facilities in the United States. We heard Congressman Franks speak eloquently about the risk of solar flares, again, something we take very, very seriously. But Mr. Chairman, looking at you and the ranking member, the States that you are from as well as other States represented here, I would like to turn for a moment to the New Madrid fault and the threat that earthquakes pose as sort of a representative way of looking at the nature of natural hazards. In the national-level exercise we just conducted 2 weeks ago that posited for its scenario a 7.7 earthquake on the New Madrid fault, our friends at NERC estimated that there would be a multi-State long-term power outage, long term, weeks, potentially months, rolling blackouts in Chicago and in the East Coast, and what I would like you to think about is the

downstream effects of such an event, both on critical Department of Defense operations in Fort Campbell, for example, everyplace else, all the facilities are represented here today, but also in the immediate area. Two things to think about. First of all, the way that the loss of electric power would magnitude the scale of the catastrophe to which we would all be responding. Municipal water systems in Memphis and elsewhere, they depend on the flow of commercial power. When that power stops, drinking water gradually gets turned off, and in a situation like the New Madrid fault, gas lines are going to be broken, fires are going to be breaking out, where is the water pressure to fight those fires. Where is the gas to fuel the trucks that will be going to fight the fires or collect water elsewhere, because of course as you all know, gas pumps and diesel pumps, they run on electric power. We would very quickly be in a situation where we need to get emergency diesel power flowing to nuclear power plants, State emergency operations centers, everything else required to deal with the disaster, and this would be in a situation where roads and bridges are down and there is so much demand for backup diesel power compared to the amount of diesel fuel that is prepositioned at these facilities.

These are examples of the kinds of ways in which a disaster would be magnified but I am looking at it from an additional perspective. The Department of Defense would be supporting the governors of your States through FEMA, of course, and there would be big demand on the Department of Defense to provide additional support at the same time that our response operations would be severely disrupted. With the loss of electric power, how are we going to receive the massive forces that would be coming in at the request of governors? How are we going to stage them, move them forward? These are challenges that we need to take on very, very seriously.

Now, the Department of Defense is doing so, and what I wanted to do briefly is talk about some of the remediation efforts we are taking. First of all, we are working closely with the Department of Energy to partner together in the Federal Government so we can reach out to industry and find out how we can work together with industry to provide industry with what we would call a better design basis to ensure the resilience of the electric power grid against all of these hazards. I believe today's power grid has very strong resilience but it is not designed for the kinds of threats that we are talking about today, above all, cyber or carefully designed kinetic attacks. We need to work together with industry to find a way to enable them to build more resilience into the grid and then inside the Department of Defense family, we need to do a better job of securing the flow of electric power to our critical defense facilities in all of the States represented here today to make sure that single points of failure on the flow of electric power coming in, we take care of those problems and we remedy those in partnership with the utilities in the same neighborhoods as our military facilities.

Mr. Chairman, I look forward to answering your questions.

[The prepared statement of Mr. Stockton follows:]

Testimony of the Honorable Paul Stockton
Assistant Secretary of Defense
Homeland Defense and Americas' Security Affairs
Department of Defense

Before the Subcommittee on Energy and Power
The Committee on Energy and Commerce
United States House of Representatives
May 31, 2011

Mr. Chairman and Members of the Committee:

I would like to begin by thanking you for the opportunity to testify today and for your interest in the security of the commercial electric power grid. I appreciate the vital role of Congress in the realm of energy security. Your leadership and leadership is critically important.

Also, I would like to thank two highly-valued and essential interagency partners: the Office of Electricity Delivery and Energy Reliability at the Department of Energy under Assistant Secretary Pat Hoffman; and the Office of Infrastructure Protection at the Department of Homeland Security under Assistant Secretary Todd Keil.

On this issue of great importance to the security of our nation, the Department of Defense is largely in a supporting role. The Department of Energy, the lead agency on energy matters, and the Department of Homeland Security, the lead agency for Critical Infrastructure Protection are in the lead. However, the Department of Defense is a significant stakeholder, and the Department's ability to perform its national security functions is largely dependent upon the reliability and resilience of the commercial electric power grid.

Department of Defense Reliance and Vulnerabilities

The Department of Defense relies on commercial electric power for nearly 99% of its power needs at military installations. Worldwide force deployment, support and sustainment, including that in Iraq and Afghanistan, are heavily dependent on commercial electrical infrastructure and associated supply chains. Since the events of September 11, 2001, many Department of Defense installations have changed and expanded their roles to include current operations "reach back"

in direct support of warfighting missions. A number of installations also serve as bases of operations to support Federal emergency relief and recovery efforts. Extended commercial power disruptions at these military installations could adversely affect power projection and homeland defense mission capability. In some cases, even short-term outages on installations can impact Department of Defense mission assurance.

The Department of Defense has limited back-up power. On-site back-up diesel generators are often used to support installation and facility continuity during short-term outages, but these generators are typically not designed to operate for extended periods. The average diesel generator and on-site fuel reserves are designed to sustain basic installation functions and critical missions for 3-7 days using fuel stored on-site. During small-scale power outages, military installations are able to manage fuel resupply through existing contingency plans – although most fuel pumping assets rely on electric power and will not operate during a power outage. However, the Department is just as reliant on diesel fuel generators as the civilian sector is and will face similar reliability and fuel issues.

In the case of a large-scale power disruption, fuel resupply on military installations could be significantly compromised due to competing demand with local and regional government and population requirements for fuel distribution. While there are existing legal authorities such as the Defense Production Act that would ensure that in such extraordinary circumstances military needs would be me large-scale power disruptions that effect military installations and our Defense Industrial Base facilities could have potentially catastrophic mission impacts that we do not yet fully understand.

Nature of the Threat

The commercial electric power grid is increasingly threatened by a convergence of challenges that could lead to electric power disruptions that have the potential to challenge our nation's defense capabilities. This complex risk environment includes: disruptive or deliberate attacks, either physical and cyber in nature; natural hazards such as geomagnetic storms, and natural disasters with cascading regional and national impacts; long supply chain lead times for key replacement electric power equipment; increases in energy demand surpassing production and distribution; aging infrastructure; and transition to automated control systems and other smart grid technologies.

Mr. Chairman, I am going to refrain from speaking in any more detail on the nature of our adversarial threats, but please allow me to share a couple of examples related to the impacts natural disasters can have on the Department of Defense. The threat posed by space weather events is a serious challenge to our national security. A strong electromagnetic pulse from a solar storm can fuse the copper wires of high-voltage transformers, damaging them beyond repair. The National Academies of Science reports that if solar storms occurred today comparable to those that took place in the United States in 1921, more than 350 transformers could suffer permanent damage, leaving as many as 130 million people without power. While it is difficult to project the probability of such events, extended power outages at Department of Defense installations would significantly affect the Department of Defense's execution of key missions, both here in the United States and overseas. Projection of military force overseas and homeland defense mission capability is heavily dependent on commercial critical infrastructure and supply chains, which all rely on the electric grid for power. Large-scale power disruptions could also have significant impact on our defense support of civil authorities' mission. There would be substantial calls for National Guard support to basic public safety functions and human needs. This would be the federal government, and Department of Defense's priority. One particular area of concern is our ability to receive and stage our consequence management forces due to the loss of power and damage to the communication and transportations sectors.

This year's National Level Exercise was based on a major earthquake scenario that occurs along the New Madrid Seismic Zone. The initial 7.7 magnitude earthquake and subsequent 6.0 magnitude earthquake would cause extensive damage to the electric grid across several States. The first quake would instantly de-energize approximately 750 transmission lines and 300 substations. This would likely affect 100-150 million people, with the Northeast, Southwest and Midwest experiencing most of the outages. Many areas of the Eastern Interconnection would have down times of at least 14 hours to 5 days. Areas suffering physical damage could have much longer down times ranging into weeks and months depending on damage to long lead-time items like transformers and towers. According to an electricity sector damage assessment by the North American Electric Reliability Corporation approximately half the 500kV substations in Tennessee would be considered "Extensively Damaged". For Arkansas, at least half the 500kV and a significant portion of the 230kV substations would be "Extensively Damaged". The New Madrid quake would cause one of the largest electrical pathways to be interrupted, and likely cause complete destruction of multiple substations.

We simply don't understand the potentially cascading effect that could result from a large-scale, long-term loss of electric power. The bottom line is that we are not where we need to be in really understanding how all of these components are interconnected.

Interagency and Industry Collaboration

The Department of Defense fully recognizes the strategic importance of mitigating the growing risks to the commercial electric power grid, and therefore, the Department is taking affirmative steps internally and externally. Senior leaders are re-focusing some of the Department's energy security efforts.

Although there are steps the Department can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical Department of Defense missions is not something the Department of Defense can do acting alone. Meeting and securing the Department of Defense's critical electric power needs in an interdependent and increasingly complex risk environment requires a broad scope of collaborative engagement between government and industry stakeholders whose roles and responsibilities in power grid security and resiliency are distributed and shared. While there are maintenance and on-site power surety efforts that need some new focus, for the Department of Defense to succeed in this challenge, leadership and support from industry representatives and interagency partners at various levels of government are imperative.

The Department of Defense is collaborating with the Department of Energy, the Department of Homeland Security, the Federal Energy Regulatory Commission and industry representatives, namely the North American Electric Reliability Corporation, in these matters. For example, we are planning to develop a combined kinetic and cyber threat-based scenario for the U.S. electric power grid that could be applied on a regional scale throughout the country and be used to support the development of a new system "design basis" for building additional resilience in the U.S. electric power grid. We are also working with the North American Electric Reliability Corporation on planning a case study of a military installation for analysis, paired up with the local utility provider to determine what can be done in the short-term to mitigate electric power vulnerabilities and risks. The Department is also participating in exercises such as the recent National Level Exercise-11 exercise and upcoming Departments of Homeland Security, Energy and Defense sponsored Secure Grid 2011 and the North American Electric Reliability Corporation's GridEx 2011.

These partnerships will help the Department of Defense achieve greater energy grid security and resiliency and help mitigate the risks to critical Department of Defense installations and facilities of commercial power outages.

Department of Defense Efforts Underway

The Department of Defense is making organizational changes and capability improvements that address electric power reliability and security issues and that enable better risk-informed decision-making and investments.

This year the Department of Defense submitted a report to Congress under Section 335 of the 2009 National Defense Authorization Act. Section 335 requires the Department to submit an annual report to Congress on efforts to mitigate the risks posed to Department of Defense mission critical installations, facilities, and activities by extended power outages resulting from failure of the commercial electricity supply or grid and related infrastructure. Congress enacted Section 335 of the National Defense Authorization Act in response to the publication of a 2008 Report by the Defense Science Board on the Department of Defense Energy Strategy, titled "More Fight, Less Fuel." The report found that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid" upon which Department of Defense overwhelmingly relies for its electrical power supplies.[1]

I would like to highlight several Department of Defense initiative that serve to foster improvements in electric grid security.

Energy Grid Security Executive Council

The 2008 Defense Science Board Report recommended that the Department of Defense establish an interagency oversight group on commercial electric grid issues because within the Department of Defense, there is no central authority on energy security matters. Energy security roles and responsibilities are widely distributed, with different entities managing security against physical, nuclear, and cyber threats, cost and regulatory compliance, and the response to natural disasters. More than a year ago, the Department of Defense established the Energy Grid Security Executive Council. The Energy Grid Security Executive Council brings

[1] Report of the Defense Science Board Task Force on Department of Defense Energy Strategy, *"More Fight – Less Fuel"*, February 2008

together experts and senior executives from across the Department of Defense and the Departments of Energy and Homeland Security to focus on ensuring the security of the electric grid that serves the Department of Defense. The Energy Grid Security Executive Council focuses on the Department's energy grid vulnerability issues, the risk to critical missions created by commercial power outages, and developing comprehensive mitigating solutions.

Further, the Energy Grid Security Executive Council helps identify gaps and deficiencies and recommended approaches to secure access to adequate and reliable energy sources necessary to ensure continuity of critical defense missions in the event of extended failure of commercial energy infrastructure. The Energy Grid Security Executive Council makes use of existing Department of Defense legal and budgetary authorities and seeks to achieve greater electric grid security through development, coordination and oversight of policies, strategies, plans and initiatives.

Homeland Defense Energy Security Case Studies

I initiated a series of regional Energy Security Case Studies in January 2010 to address the policy and technical issues necessary to mitigate the risks of long-term electric power outages to clusters of Department of Defense and Defense Industrial Base sites. The Energy Grid Security Executive Council provides oversight of this effort. The case studies are consistent with requirements under Section 335 of the 2009 National Defense Authorization Act and a 2008 Defense Science Board Report recommendation that the Department of Defense take actions to "island" installations from the commercial electric power grid. [2]

The case studies are an attempt to analyze the impact of an extended power outage and the potential range of feasible Department of Defense and interagency solutions, much like an analysis of alternatives. The studies are intended to help set the stage for defining the size and scope of the issue and to help facilitate the requirements process. They will help define where Department of Defense's prudent investments should end and where commercial and civil authorities, responsibilities and investments should begin. The case studies approach is designed to provide greater electric power security to a region by separating key elements of generation and distribution infrastructure from the grid as an independent operating unit or "island". The island would be capable of generating

[2] Report of the Defense Science Board Task Force on Department of Defense Energy Strategy, "More Fight – Less Fuel", February 2008

and distributing electric power if the grid (outside the region) is disrupted for either short or extended periods of time.

The first of three Case Studies was initiated in May 2010 in the Norfolk, Virginia region. The Navy's Dahlgren Mission Assurance Division completed the assessment phase (the first of three phases) for the Norfolk case study on May 13th. The Norfolk Region Assessment Phase recommended two risk mitigation approaches for operating electrical systems in support of the identified critical Department of Defense missions for extended electrical power outages.

The two mitigation approaches identified include working with the local utility to establish a load management schematic to ensure both critical Department of Defense and non-Department of Defense assets (such as life safety and supporting infrastructure) have sustained stable power in the event the load exceeds available generation. The study also recommends a second approach that separates the mission critical functions, those identified during the mission analysis, from the commercial grid and establishes separate microgrids using an integrated network of back-up generators on the installation. This enable Department of Defense to manage the load and generation within the microgrids, ensure constant and stable power to critical Department of Defense missions and reduce the overall load in the region providing the utility provider with additional flexibility stabilizing the grid and providing power to the community. Pursuing both mitigation approaches optimizes management of electric power for critical Department of Defense missions, supporting infrastructure and broader community needs. There are several potential options for finding a balance between commercially-generated and government-generated power on the installations that will be explored.

The Mission Assurance Division recently initiated phase II (solutions refinement) to refine the recommended mitigation approaches and develop a technically relevant and feasible mitigation plan. A second case study is underway at Vandenberg Air Force Base in California, with a set of preliminary findings and recommendations due in July 2011. A third case study is in the initial planning stages and will include a cluster of Defense Industrial Base facilities in Texas.

All case studies are pursuing the goal of mitigating the risks to Department of Defense missions caused by long-term electric power outages. The end state is a comprehensive, adaptable, and repeatable methodology to identify high-order commercial electric power-related risks on a regional basis throughout the United States and develop and implement appropriate mitigation solutions.

Marine Corps Air Ground Combat Center Base Twentynine Palms

At Twenty Nine Palms, a Marine base in the Mojave Desert, we are demonstrating new micro-grid technology—a system of self-generated electricity and intelligent controls that can be operated independently if the commercial grid goes down. Micro-grids improve energy efficiency, make it easier to incorporate solar and wind power, and ensure power can be directed to facilities that need it most. Most importantly, they reduce the vulnerability of our power supplies to disruption.

The remote base in the Mojave Desert serves a population of more than 27,000 military and civilian personnel who facilitate large scale training and exercises. The austere conditions, limited infrastructure and continuity of operations place a heavy demand on the base's electrical infrastructure. The California base sustains its mission with over 10MW of power generated on site by a 2MW solar photovoltaic farm, 1MW of solar photovoltaic shading, a 0.5MW fuel cell and a 7.2 MW Cogeneration plant. The base is tying together its disparate electrical infrastructure in an optimal way while serving as a test bed for new technologies through various Department of Defense initiatives including the Environmental Security Technology Certification Program. The centerpiece of the facilities electrical infrastructure integration is being implemented to demonstrate how microgrids will serve as an important component of the Smart Grid.

Key features of the Twentynine Palms microgrid include centralized supervisory control, distributed metering and a secure wireless network to create a self-contained system capable of unplugging from the utility grid. The microgrid is a smart power distribution system that both manages and optimizes the flow of electricity around the base. The microgrid is particularly adept at dealing with the variability of intermittent renewable energy generation, combining it with energy storage and ensuring power quality and reliability. Additionally, the microgrid addresses the demand side of the energy system and sheds loads when needed.

Demonstration projects like the Twentynine Palms microgrid aim to increase energy security on Department of Defense installations, while reducing energy consumption and managing electricity usage more effectively. Many military installations, like Twentynine Palms, will serve as examples of how communities and campuses can develop their own microgrids. Remote communities in particular will look to facilities like Twentynine Palms for insights and best practices.

Energy Surety Microgrid

The Department of Energy currently funds an effort at Sandia National Laboratory to investigate new approaches for secure and robust power sources near critical loads and ways to better manage existing power generation and loads to improve the reliability and security of electric power at military installations. The Sandia approach, called the Energy Surety Microgrid, is an alternate energy delivery methodology developed to ensure that the reliability of the electric infrastructure at a given military facility will fully satisfy critical mission needs. The Sandia Energy Surety Microgrid methodology identifies buildings and operations at military facilities that are mission critical, and creates a secure and reliable power system to support these missions for the durations required.

Demonstration of Electric Grid Security Architecture

Building on the Sandia Energy Surety Microgrid project, U.S. Pacific Command and U.S. Northern Command proposed a comprehensive microgrid candidate demonstration of a cyber-secure electric grid security architecture in partnership with the Departments of Energy and Homeland Security. The demonstration plans to include cyber-secure smart microgrids with demand side management and integration of renewable energy and energy storage on military installations for improved mission assurance during prolonged outages of commercial power. The demonstration would also include integration of cyber-secure industrial control systems; application of Smart Grid technologies; distributed and variable renewable generation and energy storage; and redundant, distributed back-up power generation.

The application of cyber-secure smart microgrids on military installations would not replace commercial power as a primary source, but would enable reliable, secure, and sustainable backup power for critical missions at the installation level. The results of the demonstration would help inform infrastructure investment decisions needed to reduce the risk of extended electric power outages to military installations and potentially, the surrounding civilian communities.

Conclusion

Mr. Chairman, I would like to close by emphasizing that continued leadership and support from Congress, our lead Federal agencies and industry is

imperative for the Department of Defense to succeed in achieving greater electric grid security for Department of Defense installations and critical missions.

I would like thank you again for the opportunity to testify today and for your interest in the security of the commercial electric power grid.

With the assistance of its partners, the Department of Defense will continue actively test energy security and resiliency solutions, and to implement short, medium, and long-term plans and mitigation actions necessary to secure critical missions.

Thank you, and I very much look forward to your questions.

Mr. WHITFIELD. Thank you, Mr. Stockton.

Mr. McClelland, you are recognized for a 5-minute opening statement.

STATEMENT OF JOSEPH H. MCCLELLAND

Mr. MCCLELLAND. Thank you. Mr. Chairman and members of the committee, thank you for the privilege to appear before you today to discuss the security of the power grid. My name is Joe McClelland and I am the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. I am here today as a commission staff witness, and my remarks do not necessarily represent the views of the commission or any individual commissioner.

In the Energy Policy Act of 2005, Congress entrusted the commission with a major new responsibility: to oversee mandatory, enforceable reliability and cybersecurity standards for the Nation's bulk power system. This authority is in section 215 of the Federal Power Act. It is important to note that FERC's authority under section 215 is limited to the "bulk power system," which excludes Alaska and Hawaii, transmission facilities in certain large cities such as New York, as well as local distribution systems. Under section 215, FERC cannot author or modify reliability or cybersecurity standards but must depend upon an electric reliability organization, or ERO, to perform this task. The commission selected the North American Electric Reliability Corporation, or NERC, as the ERO. The ERO develops and proposes cybersecurity standards or modifications for the commission's review, which can then either approve or remand. If the commission approves the proposed cybersecurity standard, it becomes mandatory in the United States, applying to the users, owners and operators of the bulk power system. If the commission remands a proposed standard, it is sent back to the ERO for further consideration.

Pursuant to its responsibility to oversee the reliability and cybersecurity of the power grid, in January of 2008 FERC approved eight cybersecurity standards known as the critical infrastructure protection, or CIP standards, but also directed NERC to make significant modifications to them. Compliance with these eight CIP standards first became mandatory on July 1, 2010. Although NERC has filed and the commission has approved some modification to the CIP standards, the majority of the commission's directed modifications to the CIP standards have not yet been addressed by NERC. It is not clear how long it will take for the CIP standards to be modified to eliminate some of the significant gaps in protection within them.

On a related note, as smart grid technology is added to the bulk power system, greater cybersecurity protections will be required, given that this technology provides more access points thereby increasing the grid's vulnerabilities. The cybersecurity standards will apply to some but not most smart grid applications.

Moreover, there are non-cyber threats that also pose national security concerns. Naturally occurring events or physical attacks against the power grid can cause equal or greater destruction than cyber attacks, and the Federal Government should have no less ability to protect against them. One example is electromagnetic

pulse, or EMP. An EMP event could seriously degrade or shut down a large part of the power grid. In addition to manmade attacks, EMP events are also naturally generated, caused by solar flares disrupting the earth's magnetic field. Such events are inevitable, can be powerful, and can also cause significant and prolonged disruptions to the grid. In fact, FERC, DHS and DOE recently completed a joint EMP study through the Oak Ridge National Laboratory. The study evaluated both manmade and naturally occurring EMP events to determine their effects on the power system and to identify protective mitigation measures that could be installed. Included among its findings was that without effective mitigation, if the solar storm of 1921, which has been termed a one-in-100-year event, were to occur today, well over 300 extra high-voltage transformers could be damaged or destroyed, thereby interrupting power to 130 million people for a period of years. Although section 215 of the Federal Power Act can provide an adequate statutory foundation for the development of routine reliability standards for the bulk power system, a threat of cyber attacks or other intentional malicious acts against the electric grid is different. These are threats that can endanger national security that may be posed by criminal organizations, terrorist groups, foreign nations or others intent on attacking the United States through its electric grid. Widespread disruption of electric service can quickly undermine our government, our military, our economy as well as endanger the health and safety of millions of our citizens. Given the national security dimension to this threat, there may be a need to act quickly, to act in a manner where action is mandatory rather than voluntary and to protect certain information from public disclosure. Faced with a cyber 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. The commission's legal authority is inadequate for such action.

New legislation should address several key concerns. First, FERC should be permitted to take action before a cyber or physical national security incident has occurred. Second, FERC should be allowed to maintain appropriate confidentiality of security-sensitive information. Third, the limitations of the term "bulk power system" should be understood as our current jurisdiction under 215 does not apply to Alaska and Hawaii as well as some transmission facilities and all local distribution facilities. Fourth, entities should be able to recover costs if they occur to mitigate vulnerabilities and threats. And finally, any legislation on national security threats to reliability should cover not only cybersecurity threats but also natural events and intentional physical malicious acts including threats from an EMP. The GRID Act draft addresses many of these issues.

Thank you for your attention today, and I look forward to any questions that you may have.

[The prepared statement of Mr. McClelland follows:]

Testimony of Joseph McClelland

Director, Office of Electric Reliability

Federal Energy Regulatory Commission

Before the Committee on Energy and Commerce

Subcommittee on Energy and Power

United States House of Representatives

May 31, 2011

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to appear before you to discuss the security of the electric grid. My name is Joseph McClelland. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). The Commission's role with respect to reliability is to help protect and improve the reliability of the Nation's bulk power system through effective regulatory oversight as established in the Energy Policy Act of 2005. I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act (FPA) and the Commission's implementation of that authority with respect to cyber related reliability issues primarily through Order No. 706. I also will describe some of the current limitations in Federal authority to protect the grid against physical and cyber threats, and also comment on the GRID Act.

Background

In the Energy Policy Act of 2005 (EPAct 2005), 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 Electric Reliability Organization (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 Commission has certified the North American Electric Reliability Corporation (NERC) as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States 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." The Commission itself does not have authority to modify proposed standards. Rather, 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 ERC to submit a proposed standard or modification on a specific matter but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Limitations of Section 215 and the Term "Bulk Power System"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. The Commission recently issued Order No. 743, which directs NERC to revise its interpretation of the bulk power system to eliminate inconsistencies across regions, eliminate the ambiguity created by the current discretion in NERC's definition of bulk electric system, provide a backstop review to ensure that any variations do not compromise reliability, and ensure that facilities that could significantly affect reliability are subject to mandatory rules. NERC is currently developing its response to that order. However, it is important to note that section 215 of the FPA excludes local distribution facilities from the Commission's reliability jurisdiction, so any revised bulk electric system definition developed by NERC will still not apply to local distribution facilities.

Critical Infrastructure Protection Reliability Standards

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber related reliability issues. In August 2006, NERC submitted eight proposed cyber 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." Under NERC's implementation plan for the CIP standards, full compliance became mandatory on July 1, 2010.

On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The Commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the Commission into phases, based on their complexity. NERC opted to resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 CIP standards and directed NERC to develop additional modifications to certain of them. Pursuant to the Commission's September 30, 2009 order, NERC submitted Version 3 of the CIP standards which revised Version 2 as directed. The Version 3 CIP standards became effective on October 1, 2010. This first phase of the modifications directed by the Commission in Order No. 706, which encompassed both Version 2 and Version 3, did not modify the critical asset identification process, a central concern in Order No. 706.

On February 10, 2011, NERC initiated the second phase of the Order No. 706 directed modification, filing a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. This filing is currently under review by the Commission. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which accommodates an extension of time requested by NERC.

The remaining CIP standards revisions to respond to the Commission's directives issued in Order No. 706 are still under development by NERC. It is important to note that the majority of the Order No. 706 directed modifications to the CIP standards have yet to be addressed by NERC. Until they are addressed, there are significant gaps in protection such as a needed requirement for a defense in depth posture. NERC's standards development plan filed with the Commission in April 2011 classifies these outstanding revisions to the CIP standards as "High Priority" with a targeted completion in the second quarter of 2012.

Identification of Critical Assets

As currently written, the CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the requirements of the standards. In Order No. 706, the Commission directed NERC to revise the standards to require 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. This revision to the standards, like all revisions, is subject to approval by the affected stakeholders in the standards development process. NERC has attempted to address this directive in Version 4 of the CIP standards, which is now under review by the Commission. Because it is currently under review, I cannot address its merits at this time.

When, in Order No. 706, the Commission approved Version 1 of the CIP reliability standards, it also required entities under those standards to self-certify their compliance progress every six months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP-002-1. As the Commission stated in Order No. 706, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at

maintaining the reliability of the bulk power system. The results of NERC's self-certification request showed that only 29% of responding generation owners and operators identified at least one critical asset, while about 63% of the responding transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009.

NERC conducted another self-certification survey of responsible entities to determine progress towards identification of critical cyber assets. It gathered information about critical assets and critical cyber assets as of December 31, 2009. This survey included additional questions designed to obtain a better understanding of the results from industry's critical asset identification process. In general, this survey did not demonstrate a significant increase in identified critical assets. NERC noted some encouraging results as well as some that were a cause for concern. In addition, the Regional Entities have been performing audits which have included registered entities' determination of their critical cyber asset lists. FERC staff has been observing selected audits to examine the Regional Entities' methods of conducting these audits. It is important to note that although "critical assets" are used to identify subsequent "critical cyber assets," only the subset of "critical cyber assets" are subject to the CIP standards.

NERC's Critical Infrastructure Protection Committee released a guidance document to assist registered entities in identifying their critical assets. That document, which took effect on September 17, 2009, provides "guidelines" that define which assets should be evaluated, provides risk-based evaluation guidance for determining critical assets, and describes reasonable bases that could be used to support that determination. A second NERC security guideline regarding critical cyber assets became effective on June 17, 2010. This security guideline "provides guidance for identifying Critical Cyber Assets by evaluating potential impacts to 'reliable operation' of a Critical Asset." Neither of these guidance documents contained any actions that were mandatory for users, owners or operators of the bulk-power system.

Version 4 of the CIP standards, which are currently pending before the Commission, would change the way in which critical assets are identified. Instead of using a loosely defined risk-based assessment methodology, CIP-002 Version 4 Attachment 1 contains what NERC describes as "uniform criteria for the identification of Critical Assets." For example, criterion 1.1 would identify generation plants equal to or greater than 1500MW as critical assets. The filing asserts that this would account for 29% of the installed generator capacity in the United States. Because this is an on-going proceeding before the Commission, I am limited in what I can discuss about the merits of NERC's petition.

The NERC Process

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be 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. However, the NERC process typically requires years to develop standards for the Commission's review. In fact, the CIP standards approved by the Commission in January 2008 took approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for stakeholder comment, are open, and are generally based on the procedures of the American National Standards Institute. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in its responsiveness to the Commission's directives. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. NERC-approved standards are then submitted to the Commission for its review.

The procedures used by NERC are appropriate for developing and approving routine reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process can be a strength of the process. However, it can be an impediment when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information. The current 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, while the reliability standard procedures take too long to implement efficient and timely corrective steps. On September 3, 2010, FERC approved a new reliability standards process manual filed by NERC. While this manual includes a process for developing a standard related to a confidential issue, the new process is untested and it is unclear how the process would be implemented.

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 exists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice. Moreover, faced with a 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 even 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, could widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, a reliability standard submitted to the Commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not directly modify a proposed reliability standard under section 215 and must either approve or remand it, FERC 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.

This concern was highlighted in the Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security." The audit report identified concerns regarding the adequacy of the CIP standards and the implementation and schedule for the CIP standards, and concluded that these problems exist, in part, because the Commission's authority to ensure adequate reliability of the bulk electric system is limited. This report emphasizes the need for additional authority to ensure adequate cyber security over the bulk electric system.

Finally, the open and inclusive process required for standards development is not consistent with the need to protect security-sensitive information. For instance, a formal request for a new standard would normally detail the need for the standard as well as the proposed mitigation to address the issue, and the NERC-approved version of the standard would be filed with the Commission for review. This public information could help potential adversaries in planning attacks.

Smart Grid

The need for vigilance will increase as new technologies are added to the bulk power system. For example, smart grid technology promises significant benefits in the use of electricity. These include the ability to better manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.

Smart grid applications will automate many decisions on the supply and use of electricity to increase efficiencies and ultimately to allow cost savings. Without adequate protections, however, this level of automation may allow adversaries to gain access to the rest of the company's data and control systems and cause significant harm. Security features must be an integral consideration when developing smart grid technology and must be assured before widespread installation of new equipment. 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.

Regarding data, there are multiple ways in which smart grid technologies may introduce new cyber vulnerabilities into the system. For example an attacker could gain access to a remote or intermediate smart grid device and change data values monitored or received from down-stream devices, and pass the incorrect data up-stream to cause operators or automatic programs to take incorrect actions.

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed generation sources to turn off during periods when load is approaching generation capacity, causing instability and outages on the bulk power system. One of the potential capabilities of the smart grid is the ability to remotely disconnect service using advanced metering infrastructure (AMI). If insufficient security measures are implemented in a company's AMI application, an adversary may be able to access the AMI system and could conceivably disconnect every customer with an AMI device. If such an attack is widespread enough, the resultant disconnection of load on the distribution system could result in impacts to the bulk power system. If an adversary follows this disconnection event with a subsequent and targeted cyber attack against remote meters, the restoration of service could be greatly delayed.

In addition to any smart grid related standards that may be adopted by the Commission, the CIP standards will apply to some, but not most, smart grid applications. The standards require users, owners and operators of the bulk power system to protect cyber assets, including hardware, software and data, which would affect the reliability or operability of the bulk power system. These assets are identified using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a smart grid device were to control a critical part of the bulk power system, it should be considered a critical cyber asset subject to the protection requirements of the CIP standards. However, this designation is currently up to the affected entity as part of its self-determination of critical cyber assets, as discussed previously.

Many of the smart grid applications will be deployed at the distribution and end-user level and as such the CIP standards, as they are currently written, may not apply. However, as discussed above, these applications either individually or in the aggregate could affect the bulk power system.

Physical Security And Other Threats To Reliability

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. EMP events can be generated from either naturally occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents. This effect, also termed the "E3" component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area. Regarding man-made events, EMP can also be generated by weapons. Equipment and plans are readily available that have the capability to generate high-energy bursts, termed "E1", that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets. The most comprehensive man-made EMP threat is from a high-altitude nuclear explosion. It would affect an area defined by the "line-of-sight" from the point of detonation. The higher the detonation the larger the area affected, and the more powerful the explosion the stronger the EMP emitted. The first component of the resulting pulse E1 occurs within a fraction of a second and can destroy control and communication electronics. The second component is termed "E2" and is similar to lightning which is well-known and mitigated by industry. Toward the end of an EMP event, a third element, E3, occurs. This causes the same effect as solar magnetic disturbances. It can damage or destroy power transformers connected to long transmission lines. It is important to note that effective mitigation against solar magnetic disturbances and non-nuclear EMP weaponry provides effective mitigation against a high-altitude nuclear explosion.

In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] Both electrical equipment and control systems can be damaged by EMP.

---

[1] Graham, Dr. William R. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2004).
[2] Dr. John S., Jr. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2008).

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because semiconductor technology did not exist at the time. Were the storm to happen today, according to an article in *Scientific American*, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[3] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the *Scientific American* article, and the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages. The power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced currents. The damage or destruction of numerous transformers across the country would result in reduced grid functionality and even prolonged power outages.

In March 2010, Oak Ridge National Laboratory (Oak Ridge) and their subcontractor Metatech released a study that explored the vulnerability of the electric grid to EMP-related events. This study was a joint effort contracted by FERC staff, the Department of Energy and the Department of Homeland Security and expanded on the information developed in other initiatives, including the EMP commission reports. The series of reports provided detailed technical background and outlined which sections of the power grid are most vulnerable, what equipment would be affected, and what damage could result. Protection concepts for each threat and additional methods for remediation were also included along with suggestions for mitigation. The results of the study support the general conclusion that EMP events pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

The existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure.

The Need for Legislation

In my view, section 215 of the Federal Power Act provides an adequate statutory foundation for the ERO to develop most reliability standards for the bulk power system. However, the nature of a national security threat by entities intent on attacking the U.S. through vulnerabilities in its electric grid stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as

[3] Odenwald, Sten F. and Green, James L., *Bracing the Satellite Infrastructure for a Solar Superstorm*, Scientific American Magazine (Jul. 28, 2008).

vegetation management and protective relay maintenance practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as 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.

The Commission's current legal authority is inadequate for such action. This is true of both cyber and physical threats to the bulk power system that pose national security concerns. Section 215 of the FPA excludes all facilities in Alaska and Hawaii and all local distribution facilities from the Commission's reliability jurisdiction, which may leave significant facilities vulnerable to the threat of a cyber or physical attack. In addition, although the NERC standards development process as envisioned in section 215 can be fine for routine reliability matters, it is too slow, too open and too unpredictable to ensure its responsiveness in the cases where national security is endangered. This process is inadequate when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information.

These shortcomings can be solved through a comprehensive, government-wide approach to cyber security issues or through a sector-specific approach. If a government-wide course is pursued, care should be taken to ensure that the two approaches complement each other, preserving FERC's ability to regulate effectively under legislation such as the GRID Act. The GRID Act would authorize FERC to address cyber security vulnerabilities of the Nation's critical electric infrastructure. The GRID Act does not preclude or discourage FERC from working with other agencies or even a central authority (if Congress or the President elects to establish one as envisioned by other proposed legislation) to address and mitigate these issues. In fact, in order to be most effective, the Commission would need to coordinate closely with other agencies and bring all resources and expertise to bear on the particular vulnerability or threat presented. FERC already works closely with agencies such as DOE, DOD, DHS, NSA, FBI, NRC, and CIA in these matters and expects to continue to do so if the proposed legislation is passed, even in combination with other cyber security legislative efforts affecting other industries and agencies.

Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the federal government to take action before a cyber or physical national security incident has occurred. In my opinion, the GRID Act addresses this concern by allowing the Commission to timely act on imminent grid security threats, as determined by the President, before an incident occurs and by giving the Commission authority to issue orders for emergency measures to protect the reliability of the bulk power system or defense critical electric infrastructure. In addition, the GRID Act would allow the Commission to promulgate a rule or issue an order requiring owners, operators and users of the bulk power system to implement measures to protect to bulk power system against a grid security vulnerability. In particular, the federal government should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action.

Second, any legislation should ensure appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack. The GRID Act also includes provisions for protection of critical electric infrastructure information, which includes a provision for FERC to establish standards for and facilitate the appropriate sharing of protected information.

Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize Commission action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas. The GRID Act would apply only to the bulk power system or defense critical electric infrastructure, which would include defense critical electric infrastructure connected to distribution systems. As such, it would appear not to protect other distribution systems. While Alaska and Hawaii would be excluded, the GRID Act provides that the President will designate facilities located in the United States, including the territories, which are critical to the defense of the United States and vulnerable to a disruption of the supply of electric energy provided to such facility. Under the proposed GRID Act the Commission could, after appropriate consultations, promulgate rules to require the owners of such facilities to implement measures to protect the defense critical electric infrastructure against a vulnerability.

Fourth, it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats. The GRID Act requires the Commission to establish a mechanism to permit owners, operators or users to recover prudently incurred costs required to implement emergency measures taken to address grid security threats. I support this provision and any clarifications that might better ensure recovery of costs incurred under this legislation.

Conclusion

The Commission's current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. 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. The GRID Act in front of us today would go a long way to resolving this issue. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. WHITFIELD. Well, thank you all for your testimony.

Many of you heard Congressman Franks and Mr. Langevin also talk about the need to expand. I noticed the White House in their cybersecurity proposal is exactly that, is focused only on cybersecurity, and that was a suggestion that Mr. Franks made that let us do cybersecurity in one bill and let us address the other issues in a separate bill. Do you all have any thoughts as far as strategy, that that is something the committee should attempt to do, or not? Ms. Hoffman.

Ms. HOFFMAN. As was mentioned earlier, cybersecurity is a difficult and complex issue, and EMP and other issues are different in nature, although the impact to the country can be devastating, either one, so in order to tackle things one at a time, the administration is looking just comprehensively at the cyber legislation individually.

Mr. WHITFIELD. OK. Mr. Stockton, do you have a comment?

Mr. STOCKTON. Yes, sir. I think that the cyber legislation proposed by the administration is a critical step towards protection of infrastructure as a whole would greatly benefit the energy sector as well. Clearly, there are threats that we have been discussing that wouldn't be encompassed by this legislation but it is a critical building block on which we need to make progress.

Mr. WHITFIELD. Right. Mr. McClelland?

Mr. MCCLELLAND. I don't see where the administration's bill would conflict with the GRID Act. The administration's bill provides a broad umbrella to partner with industry to bring the practices to a higher level. The commission's authority under 215 doesn't have to conflict with that concept, and in fact, any further enhancement of the commission's authority or any regulatory authority may actually complement that concept.

Mr. WHITFIELD. Well, you know, Mr. Langevin pointed out the need to expand from bulk systems to expand your section 215 authority. Do all of you agree that that should be done? I am assuming you do, Mr. McClelland.

Mr. MCCLELLAND. As I pointed out in my testimony, the commission, you know, our position or my position is that the distribution systems aren't covered and so we wish to point out that if the term "bulk power system" is followed, there would be significant pieces of the power grid that would not be protected if the GRID Act passes, either from a cybersecurity or physical perspective.

Mr. WHITFIELD. Mr. Stockton, do you or Ms. Hoffman have any comments on that part?

Ms. HOFFMAN. I think it is important to take a holistic look at cybersecurity. As you look at the administration's proposal, it wants to take a comprehensive approach so that would include entities that would be defined as critical whether they are in the bulk power system or at the distribution. The important thing to note is, we need everybody to understand how to advance cybersecurity procedures and postures, and I would say that includes State governments as well as any Federal action.

Mr. WHITFIELD. How would you all describe the coordination between DOE, DOD and FERC today on these types of issues?

Ms. HOFFMAN. The coordination between DOD and DOE primarily looks at defense facilities and the interface with the energy

sector. We do provide some support work on studies and looking at the interdependency between the energy sector and the defense. We are looking at micro grids. We are looking at advanced technologies in support of the defense facilities. Our coordination with FERC provides tools and technologies to look at improved reliability for the electric sector. We do coordinate it with information sharing to the extent possible, looking at technologies that will actually improve the posture of the system. So the coordination with FERC is, they are a regulatory entity. The Department of Energy funds public-private partnerships so in a sense, we are incentivizing changes within industry, and FERC looks at regulating aspects of industry.

Mr. WHITFIELD. Does anybody else have any comment?

Mr. MCCLELLAND. I would say there are formalized mechanisms, as Ms. Hoffman pointed out. There are formalized mechanisms such as the government coordinating council, where the Department of Energy sits as the energy sector lead. FERC participates in those formalized initiatives with the other agencies. In addition, we have excellent working relationships on an informal or an impromptu basis with the Department of Energy, the Department of Defense, Department of Homeland Security, CIA, NSA and NRC. So we reach out as necessary to either borrow expertise or provide expertise pursuant to power grid and individual needs on the grid.

Mr. WHITFIELD. When we talk about cybersecurity attacks, in the United States I am not aware of any major attack, and internationally, what comes to my mind is the Stuxnet in Iran which basically shut down some of their nuclear power systems. Are you aware of any other major cybersecurity attacks that have had significant impact?

Ms. HOFFMAN. I am not aware of any major significant attacks. Stuxnet was a very complex attack within the nuclear sector. The issue or the focus that we have is, there are incidents that may occur, and we need to be prepared to be able to respond to those incidents quickly and promptly, and so as we move forward, it is looking at, how do we have an incident management plan or an incident response plan to be able to address the event quickly, so looking at information exchange, diagnostics, and the ability to deter and prevent any further damage.

Mr. WHITFIELD. OK. Mr. Rush, you are recognized for 5 minutes.

Mr. RUSH. Thank you, Mr. Chairman.

First of all, I want to thank the witnesses. In the last Congress, when we worked on this issue in a bipartisan manner, the administration provided the members of this committee with a classified briefing that helped us understand the vulnerabilities to our electric grid and actions needed to protect that same grid, and I just have to ask each of you, in light of the fact that we have some new members, a lot of new members on this subcommittee, will each of you agree to at a time determined by the chairman to return and brief the members of this committee again on the vulnerabilities of our cybersecurity area? Will each of you do that?

Ms. HOFFMAN. Yes, sir.

Mr. STOCKTON. Yes.

Mr. MCCLELLAND. Yes.

Mr. RUSH. Well, let me just ask Ms. Hoffman, you seem to feel as though, the impression that I get is that you seem to feel as though oK, this is a step in the right direction but it is narrow, and what the administration is looking at is a much broader view. They are taking a more universal, a broader view of this particular issue. If you were to overlay the administration's efforts on this bill, this proposal and the GRID Act, what would we see and what would you see as being some of the most significant differences?

Ms. HOFFMAN. The administration's proposed discussion draft focuses on several things. It looks at criminal aspects with respect to criminal charges and enforcement. It looks at voluntary information sharing. It looks at voluntary assistance. So it is building a public-private partnership to actually build capabilities in support to the industry sector, which is critically needed at this point in time. It also looks at the ability to develop plans, risk-based plans. Now, most of the critical infrastructure definition and the development of risk-based plans will of course be done through a rulemaking process through DHS, but the administration has taken a holistic approach of trying to get all the sectors up to a cybersecurity baseline performance.

Now, in deference to the GRID Act, which is focusing on transformers, EMP, it is focusing on emergency and standard development, which is a slightly different approach from what the administration's position is but both those could be worked for complementary efforts.

Mr. RUSH. Do any of the other witnesses have any comments on this?

Well, let me ask you this. It seems as though—I know my State, as I indicated earlier, yesterday the members of the general assembly passed smart grid regulations, and it seems as though some of the States are starting to move on their own, but the administration has a discussion draft or a pending bill, and I am not sure whether or not these States who are starting to take actions are basing any of their efforts on what the administration is ultimately looking at. So how much cooperation, how much sharing of information, how much enlightenment is the administration providing to these States so they won't have to come back and redo whatever legislation they might pass prior to the administration getting its bill passed, and what is the status of the administration's proposal right now? There are two points there. Ms. Hoffman? You might want to——

Ms. HOFFMAN. The status is, it is a discussion draft and the administration is looking forward to working with Members of Congress to continue that discussion, to advance the components of that discussion draft. With respect to smart grid, there are security profiles and standards that are currently under development to provide security within the devices as they are being built, so we are working cybersecurity standards with the development of device as we deploy and implement smart grid technologies.

One of the things that we are trying to do is provide improved system performance, which can aid and provide benefit for restoration time out as management so more preventive versus looking at the consequences if an event occurs.

Mr. RUSH. Gentlemen, my time is up.

Mr. WHITFIELD. Thank you, Mr. Rush.

At this time I recognize the gentleman from West Virginia, Mr. McKinley, for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman.

Ms. Hoffman, I wasn't here when this bill passed last year, but I am curious if you could walk me through it or maybe someone else on the panel perhaps. The way I am reading this, the GRID Act, is we start with subsection A of definitions and then we move into B, which is emergency response measures, and that refers very specifically to security threat, and under that subsection B, it has a subsection 6 which has cost recovery. So there is a vehicle, a mechanism to recover cost for threat. Then if we can skip C just for the moment that has to do with vulnerability, and then you go to D, which is called critical defense facilities. Under critical defense facilities, there is a subsection on page 15 about cost recovery. I am just curious, back on the one I skipped over, C, that is the section that refers to grid security vulnerabilities. Under vulnerabilities, there is no cost recovery by this particular piece of legislation. Was that intentional, that vulnerabilities would not be able to recover the costs, the utility companies and anyone else would not be able to recover their costs? I am sorry I singled you out but I don't care who answers the question.

Mr. MCCLELLAND. I can take a shot at that. I believe you are correct. I believe that threats are singled out for cost recovery. I believe under the 100 most critical facilities for the DOD, the user is required to pay for any upgrades or any enhanced measures. I didn't see cost recovery for vulnerabilities either.

Mr. MCKINLEY. Does that make any sense to you, that there is someone that could have the expense, if you read down through all the issues that you have for if nothing else the large transformer availability. There would be no way to recover the cost to having that on board.

Mr. MCCLELLAND. Right. Well, we have consistently said at the commission that we think that there must be three aspects if you would like to have someone move on one of these issues. One is, you have got to identify priorities, second, you have to identify mitigation, and third, you have to provide cost recovery.

Mr. MCKINLEY. So are you in agreement then we probably should have some cost recovery under vulnerabilities?

Mr. MCCLELLAND. Personally, I would say yes.

Mr. MCKINLEY. Do the rest of you have any problem with cost recovery under vulnerabilities?

Ms. HOFFMAN. We don't have any problem on cost recovery. Just recognize cost recovery, no matter what the actions are, is going to be recovered somewhere from the ratepayers, from the entities that are being protected. So eventually——

Mr. MCKINLEY. So if the others are very clear—I am not an attorney, I am an engineer. It just tells me when you leave something out, it looks like we have left it out deliberately.

There was another line that I caught under, I think it might have been page 8, yes, page 8 on line 22. It talks about there under cost recovery, only those that were substantial costs. Could we get that clarified somehow? Can you all help us with some language

that might be more appropriate to define what substantial costs would be?

Mr. MCCLELLAND. Sorry. Were you looking for a comment there?

Mr. MCKINLEY. Given the time, no. I hope that we can get something back on that.

The last is a little bit of concern, Ms. Hoffman, to your answer. So much of our defense is actually overseas, and we are going to be very reliant on the other countries' responses to threats and vulnerability. You said we would respond quickly. And you said you didn't know of any attack. Do we have any evidence of probing, inquiries, photography, suspicious work? Is there something going on? Because it is one thing to have an attack. The other is someone in preparation for it. Can you share any——

Ms. HOFFMAN. I just don't have any information on that.

With respect to overseas, my focus is on the domestic U.S. infrastructure so I——

Mr. MCKINLEY. What should we do then overseas if we know that is certainly a possibility with the terrorism that is going on? Do we just simply rely on the other countries to provide the same type of responses to threats and vulnerability and then we react after it has happened, or what role do you see us playing in trying to promulgate something now?

Ms. HOFFMAN. With respect to international grid structures, you know, Europe has their own sort of response mechanisms for any sort of emergency that happens on their system. I have to admit that I don't have a great insight or detail on how we should respond for an overseas issue.

Mr. MCKINLEY. I know I am running over on time. Is there some way we could maybe work something like that into here, something you could provide to us later to how we might be able to integrate both the European and the American grid together, at least in terms of cybersecurity? Thank you very much.

Mr. WHITFIELD. Did you want to respond, Ms. Hoffman?

Ms. HOFFMAN. Yes, I am willing to have further dialog. Thank you.

[The information follows:]

QUESTION FROM REPRESENTATIVE MCKINLEY

COMMITTEE:	HOUSE ENERGY & COMMERCE COMMITTEE HEARING
HEARING DATE:	MAY 31, 2011
WITNESS:	PATRICIA HOFFMAN PAGE: 61-62, LINES: 1223-1256

INSERT FOR THE RECORD

With commonality in electricity infrastructure, information networks, and global vendors, DOE recognizes that sharing lessons learned and best practices for securing the grid within our country and internationally offers an important opportunity to advance cybersecurity for the grid. DOE, along with other Federal agencies and industry organizations, currently coordinate with domestic and international partners on the development of cybersecurity standards for the grid, sharing of best practices, and mitigation solutions for identified vulnerabilities. For example, the Smart Grid Interoperability Panel (SGIP) addresses the development of smart grid standards, including cybersecurity. The SGIP 2011 summer meeting welcomed and included international participation. Additionally, DOE laboratories and subject matter experts, along with other Federal agencies such as Department of Homeland Security and the National Institute for Standards and Technology, regularly participate in international cybersecurity conferences and seminars. The Department believes it is important to continue these efforts and looks for further areas of collaboration.

The Department also participates in handling of international threat information,

including cybersecurity incidents, through several activities. The Secretary of Energy serves as a member of the National Security Council (NSC), whose members provide top level policy advice to the President and oversight in areas that include cybersecurity. The Secretary is also a member of the Homeland Security Council (HSC), which also provides top level policy oversight in cybersecurity. The Department participates on the Deputies committee of the NSC/HSC to provide policy oversight on cybersecurity, and the Department also participates on the NSC/HSC Interagency Policy Committee for the global information and communications infrastructure, a policy coordination group.

Mr. WHITFIELD. At this time I recognize the gentleman from Massachusetts, Mr. Markey, for 5 minutes.

Mr. MARKEY. Thank you, Mr. Chairman, very much. Thank you for having this very important hearing, and thanks to Mr. Franks and everyone else who is here for their interest in this issue.

Chairman Upton has continued his efforts on the bipartisan GRID Act, which I introduced with him in the last Congress. That legislation passed the Houser on suspension one year ago today, and Mr. Upton and I worked together in a bipartisan fashion to pass the bill a year ago, and I think this is a perfect example of bipartisanship because, remarkably, 99 percent of the electric energy used to power our military facilities including critical strategic command assets comes from the commercially operated grid, and over the last several years, the grid's vulnerability to cyber threats has come into sharp focus. The Department of Homeland Security revealed the so-called aurora vulnerability through which hackers could use communications networks to physically destroy electric generators, transformers and other critical assets.

Just over a week ago, Lockheed Martin suffered what it called a significant and tenacious cyber attack on its system, and in today's Wall Street Journal, a description of the Defense Department's cybersecurity plan has a military official quoted as saying that if a terrorist or other adversary shuts down our power grid, maybe we will put a missile down one of your smokestacks. Unlike the frequent outages experienced by Pepco's customers every time the Washington, D.C., area experiences a serious storm, a coordinated attack on the grid could literally shut down the U.S. economy, putting lives at risk and costing tends of billions of dollars. Damage from such an attack could take months or even years to recover from.

Moreover, from such an event may not just be a matter of rebuilding. Three nuclear reactors in Japan have suffered near-complete core meltdowns after the earthquake caused a loss of electricity needed to cool them down. Unit 1's meltdown likely began just a few short hours after the earthquake, tsunami and blackout. The hot radioactive fuel is believed to have burned holes that are as much as 10 centimeters wide through the pressure vessels. It is expected to take months to stabilize the reactors and decades to clean up the damage that the meltdown caused. And Mr. Stockton mentioned that the power outage risk associated with earthquakes near the New Madrid fault line is notable because there are extra nuclear reactors located near it, and those several reactors could be vulnerable.

So Mr. McClelland, let me ask you this. Here in the United States in the past 8 years, there have been at least 69 reports of emergency diesel generators failing at 48 nuclear reactors. Nineteen of these failures lasted for more than 2 weeks, and six lasted longer than a month, and there aren't any requirements that spent nuclear fuel pools have backup power at all when there is no fuel in the reactor core. Clearly, a blackout could cause a meltdown in this country too.

Mr. McClelland, do you believe that the portions of the grid that supply electricity to our nuclear reactors, that is, electricity to the

reactor, not from the reactor, are more secure than the rest of the grid?

Mr. MCCLELLAND. The commission has been working with the Nuclear Regulatory Commission on this issue, and there are three sources of power. There is the offsite power, that you just asked about, the on-site diesel generators——

Mr. MARKEY. So they are more secure? Are you saying they are more secure?

Mr. MCCLELLAND. There are agreements in place between the Nuclear Regulatory Commission——

Mr. MARKEY. No, but today, are they are more secure than the rest of the system, or not?

Mr. MCCLELLAND. In many cases, no.

Mr. MARKEY. No. The answer is no. Thank you.

Mr. McClelland, since the legislative hearing this committee held in October of 2009, have sufficient measures been put in place to secure the American electrical grid from cyber and physical attack?

Mr. MCCLELLAND. There has been some progress on the NERC standards, some submission as far as——

Mr. MARKEY. Have sufficient measures been put in place? "Sufficient" is the key word at this point.

Mr. MCCLELLAND. We have issued inquiries to the NERC.

Mr. MARKEY. So are you saying there are sufficient——

Mr. MCCLELLAND. There have been some filings made and we are checking the status of those filings to see whether or not they do indeed represent progress.

Mr. MARKEY. Well, let me ask you this. Given that the number of cyber access points to the grid is increasingly rapidly with the growth of smart grid applications, do you believe the threat facing the grid is greater or less than it was a year ago when the House overwhelmingly passed grid security legislation, given the fact that a smart grid actually winds up with no vulnerabilities, ironically.

Mr. MCCLELLAND. Yes, the threats are greater.

Mr. MARKEY. So you think there could be greater vulnerability?

Mr. MCCLELLAND. Undoubtedly, yes.

Mr. MARKEY. Do you believe that the way the grid security standards are currently set is even capable of leading to the rapid adoption of standards that are sufficient to respond to the threat that our grid faces?

Mr. MCCLELLAND. The commission has said on numerous occasions that when it comes to national security, the standards development process is too slow, it is too open and it is too unpredictable.

Mr. MARKEY. Mr. Stockton, do you agree with that?

Mr. STOCKTON. He is better positioned to assess the adequacy of the regulatory environment.

Mr. MARKEY. Ms. Hoffman?

Ms. HOFFMAN. There is room for improvement.

Mr. MARKEY. OK. Thank you, Mr. Chairman.

Mr. WHITFIELD. Mr. Terry, you are recognized for 5 minutes.

Mr. TERRY. Thank you.

Mr. McClelland, in the SHIELD Act versus the GRID Act, on FERC authority, do you feel that you need additional level of authority to respond to a national security threat? Can you be more

specific in that? Then on the flip side of that additional authority is how we balance that with State regulatory entities.

Mr. MCCLELLAND. The SHIELD act provides the commission with a proviso that if it finds the NERC standard insufficient, it can author a measure to put into place to address a security vulnerability. The commission currently under the 215 process cannot author or modify reliability standards. We can't author or modify NERC alerts. We can provide input but we cannot author or modify. I feel it is important that the commission be given that direct authority to be able to order interim measures or measures to be put into place, to write those measures and to direct that they put into place to address vulnerabilities to the bulk power system or threats.

Mr. TERRY. And in regard to that, do you foresee any difficulties then working with State regulatory agencies on the same issues?

Mr. MCCLELLAND. I think it is going to be very important that the commission coordinate not only with the State regulatory agencies but with the electric reliability organization and with the affected entities that the commission communicates with, so yes, I think it is very important.

Mr. TERRY. Ms. Hoffman, do you have any thoughts in regard to the additional jurisdictional request?

Ms. HOFFMAN. I think it is absolutely important for the Federal FERC to coordinate with the State entities in looking at cybersecurity vulnerabilities, mitigation measures, solutions, because as we move forward, the more educated and consistent we are across the board as we take a comprehensive approach, the more it will benefit not only the electric sector but other sectors that may have the involvement with States or other entities.

Mr. TERRY. All right. Thank you.

The other question I have in regard to the hardening of the grid, what type of hardware solutions exist out there? Would you have under the SHIELD or GRID Act the appropriate ability, authority to, for want of a better word, mandate the technology and is there any conclusions on what the costs would be nationally to adopt the hardware solutions? Mr. McClelland?

Mr. MCCLELLAND. There are several different aspects of electromagnetic pulse. If we confine the discussion to the high-altitude electromagnetic pulse from a nuclear detonation, that is a good example because it includes all three components. E1 is a high-energy radiofrequency burst. E3 is a ground-induced current. The ground-induced currents attack bulk power system transformers. They find their way onto the bulk power system transformers and destroy those transformers very quickly. One tried-and-true method is series compensation, that is to say putting capacitors in the line. That stops the flow of ground-induced current, assuming there are no parallel paths to that line.

Back to E1, it is more difficult. It is more challenging. I did receive some information recently from an Israeli scientist that shows promising technology for erecting a Faraday cage. A Faraday cage would block the E1 component, and it is simply spray-on, metallic spray-on coating that looks very promising in this area. So there is development that has been undertaken. There are others in the

world that have deployed effective mitigations against electromagnetic pulse. We have not done so in this country.

Mr. TERRY. At what cost?

Mr. MCCLELLAND. I can get back to you with those numbers. I do have those numbers but not at my fingertips. And I will just say this right up front. I think E1 is more challenging but I do have numbers also for E1 that I can get back to you.

[The information follows:]

In response to Representative Terry's questions concerning the cost of hardening the grid, Oak Ridge National Lab and an EMP Commission have both estimated the costs of mitigating EMP. The Oak Ridge National Lab issued a report in January 2010, Geomagnetic Storms and Their Impacts on the U.S. Power Grid.[1] This report estimates the average yearly cost of installing equipment to mitigate an E3 EMP (Solar type) event is estimated at less than 20 cents per year for the average residential customer.[2] This includes only material costs to provide protection on 5000 transformers and amounts to approximately $ 500 million outlay for materials.

Another estimate can be found in the April, 2008 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack "*Critical National Infrastructures*."[3] In this report, the EMP Commission has estimated the cost to mitigate E1 - EMP to be in the range of $250-$500 million for the transmission network and $ 100 - $250 million for generating plants.[4]

---

[1] Available at http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml
[2] Executive Summary at i.
[3] Available at http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf
[4] EMP Commission Report at 60-61.

Mr. TERRY. Mr. Stockton or Ms. Hoffman? Ms. Hoffman first.

Ms. HOFFMAN. I would just add to that, Joe adequately talked about some of the hardening-type activities that could be done. The other thing to keep in mind is the current state of health of the transformers. You can do some hardening, but if the current health of the transformer is not where it should be, there will be vulnerability, so also assessing the current health of the transformer will also impact to what level of deterrence or capability they have to withstand an EMP or geomagnetic solar flare. Some of the things that we need to ask is, how much do we want to harden against? Are we talking about a 200-amp thing or what is currently tested up to as an 80 amp? The other thing, do we have enough manufacturing capability of transformers in the United States? As we look at it, hardening is only one solution and there are several sets of solutions that we must keep in mind.

Mr. STOCKTON. Let me follow up. Building resilience into the system so we can provide for a rapid return of functionality, that is another alternative to hardening. We need to be able to ensure that we can from a Department of Defense perspective get back to conducting our core missions no matter what. Sometimes hardening will be the best, most cost-effective approach. Other times, quick restoration of enough power to do the bare minimum to operate those core functions, that makes better sense from a cost-effective perspective.

Mr. WHITFIELD. Ms. McMorris-Rodgers is recognized for 5 minutes.

Mrs. MCMORRIS-RODGERS. Thank you, Mr. Chairman, and thanks to all the witnesses for being here today. I appreciate your testimony. And we have certainly heard about the vulnerabilities and it suggests that there does need to be better coordination between the private sector and the government.

Commissioner McClelland and the rest of the panel, what are the standard operating procedures for an agency that has regulatory or other authority over a critical sector of our economy when a credible threat is received? For example, how does FERC communicate? Does it direct NERC to issue standards? How are those standards communicated to users of the system and what is the protocol for NERC?

Mr. MCCLELLAND. If I might start with a correction, it is Mr. McClelland. I am not a commissioner.

Mrs. MCMORRIS-RODGERS. Oh, yes, that is right.

Mr. MCCLELLAND. Thank you. I will answer your question by saying it depends on the issue. If it is an urgent matter that affects just a few entities, it may be very appropriate—and the commission has done this—to bring in members of the affected utility who have security clearances, brief them in detail on the perceived vulnerability or threat and work out a tabletop solution as to how they might increase their preparedness for some interim period of time. It wouldn't be appropriate, necessarily appropriate to try to develop a standard around a very sophisticated targeted threat that exploits a vulnerability with a handful of entities.

If it is a larger issue, the commission engages in a rulemaking procedure and so the commission would order NERC either upon a filing or upon its own motion to address a specific issue, a secu-

rity issue. NERC would then receive the order, engage industry through industry volunteers and a standards development process. That process routinely takes years. At the end of that time period, NERC would submit a standard and the commission would be in the position to either approve the standard, at which time it would become mandatory, enforceable, or to remand the standard for further work at which time NERC would take it back, consider the commission's comments and continue to pick up that issue and work on a standard.

Ms. HOFFMAN. If I may add to that?

Mrs. MCMORRIS-RODGERS. Please.

Ms. HOFFMAN. With respect to a cyber event, generally we follow the national cybersecurity response framework, but cyber events will generally be coordinated through US CERT. They will go through some analysis and forensics. They will bring the Energy Sector Coordinating Council as well as the government Coordinating Council. They will do risk and consequence analysis to determine how is that going to impact the sector, share it with the industry, the information that is available, and then be able to actually move forward with the industry's help on mitigation measures. So it is really key to having that information sharing and that quick response capability that is very important.

Mr. MCCLELLAND. May I add just one thing to that?

Mrs. MCMORRIS-RODGERS. Please.

Mr. MCCLELLAND. The only action that is mandatory is a standard. Until such time as the ERO or NERC develops a standard, submits it to the commission and it is approved, nothing is mandatory. So there are some other interim actions. NERC could issue an alert, for instance. It could be an advisory or a recommendation or an essential action. None of those would be mandatory but they do show levels of increasing urgency. NERC can convey the information to the industry, ask for a follow-up response and they communicate to the industry the importance of those levels. But outside of a standard, nothing is mandatory.

Mrs. MCMORRIS-RODGERS. Do you believe that the current system is effective, and how could it be enhanced?

Mr. MCCLELLAND. I think that the current system can be effective for routine reliability matters, tree trimming for instance, but when it comes to national security issues, these are fast-moving, very sophisticated, sometimes highly targeted situations and we have come to the conclusion that no, the standards development process is not adequate to address these types of issues. Although it can raise the bar to narrow the universe of attackers, it is not adequate in the case where national security is jeopardized to use the standards development process.

Ms. HOFFMAN. If I may add, there is room for improvement. From the perspective, we need to do a better job with respect to information sharing. That goes back to what is in the administration's comprehensive bill as well as this is looking at protection of information. That information sharing is a key critical component to getting to an effective response and mitigation measures whether it is done by the industry by themselves or it is actually looked at from a different action point of view.

Mrs. MCMORRIS-RODGERS. Thank you, everyone.

Mr. WHITFIELD. Thank you.

Mr. Olson, you are recognized for 5 minutes.

Mr. OLSON. Thank you, Mr. Chairman, and I would like to welcome the witnesses and thank you all for coming and giving us your expertise and your time.

I have got a couple of questions for you, Mr. McClelland, and you, Ms. Hoffman. Specifically, if the FERC and the DOE had to order a generating unit to operate for reliability purposes or in an emergency situation and doing so would result in that unit exceeding an environmental permit limit, would FERC or DOE indemnify the unit operator from any and all agency action or private citizen lawsuit liability?

Ms. HOFFMAN. I will get back to you for further clarification, but it is my understanding, we do not have jurisdiction over another agency's fines, penalties, regulations.

[The information follows:]

QUESTION FROM REPRESENTATIVE OLSON

COMMITTEE:	HOUSE ENERGY & COMMERCE COMMITTEE HEARING
HEARING DATE:	MAY 31, 2011
WITNESS:	PATRICIA HOFFMAN PAGE: 75-76, LINES: 1568-1578

INSERT FOR THE RECORD

Section 202(c) of the Federal Power Act provides for such orders, but does not authorize DOE to indemnify those that receive such orders. The Department is aware of only one instance where there was a possible conflict between an order issued under section 202(c) and environmental statutes. That involved Mirant Corporation (now GenOn Energy, Inc.) and its wholly owned subsidiary, Mirant Potomac River, LLC. In that instance, DOE worked closely with United States Environmental Protection Agency and state authorities to achieve both electricity reliability and protection of the environment. Under such circumstances it is the responsibility of the executive branch to administer all statutes in a manner that promotes their underlying policy goals and carefully balances any potential conflicts.

Mr. OLSON. Mr. McClelland?

Mr. MCCLELLAND. The commission has acted in conjunction with DOE on one other occasion, to my memory. It was the first time that section 207 in the Federal Power Act had been invoked. DOD invoked section 202. In that particular case, there were generating units serving the Washington, D.C., region and transmission upgrades that needed to be performed. In that case, however, both DOE and FERC did not need to conflict or clash with the environmental regulations. So I know of no case where that has already occurred but I can certainly posit that back to our general counsel and we can answer that question for you.

Mr. OLSON. Thank you for that. I just want to know, you know, what could happen? What is the realm of possibility to a company that obeys orders from you but in doing some exceeds some environmental limitations from some other agency? I mean, this is a serious problem. If you tell them to do this because there are reliability issues or emergency situations, by gosh, they are going to do that and that is the right thing to do, but certainly we don't want to have any exposure to them for doing with one arm what the government is telling them to do and the other arm says no, you guys exceeded some permitting process, we are going to punish you for doing that. I mean, again, I greatly appreciate your answers to those questions because I have had some operators back home in Texas ask me these exact questions because we have many, many natural disasters—hurricanes, tornadoes, you know, freezes, all of the above—that impacted sometimes our reliability of our grid, and I know there are differences between some of our systems in Texas but again, we do have some people out there who are very concerned about this, and I would appreciate an answer to those questions.

That is all I have. I yield back my time, sir. Thank you.

Mr. WHITFIELD. Thank you, Mr. Olson.

Thank you all very much for taking the time to come and testify. We appreciate your input and look—yes?

Mr. RUSH. Mr. Chairman, if I might, this is something that is kind of gnawing at me. I tried to get to this issue in my line of questioning. Is there an administration bill and has that bill been filed in the Senate? I know it is not in the House.

Mr. WHITFIELD. Well, they may be able to answer you. It was my understanding, and I may be wrong, that Mr. Rockefeller had introduced a bill similar to the administration's request, but maybe they can answer it.

Mr. RUSH. Is that the bill, Ms. Hoffman?

Ms. HOFFMAN. I don't have explicit knowledge. All I have right now is the discussion draft, so I am just not aware.

Mr. WHITFIELD. Do you know, Mr. Stockton?

Mr. STOCKTON. The same discussion draft.

Mr. WHITFIELD. Do you know, McClelland?

Mr. MCCLELLAND. Sorry, it is the same.

Mr. WHITFIELD. So the White House doesn't talk to you any more than it talks to us, right? We will find out.

Mr. Markey?

Mr. MARKEY. Can I just be recognized for 2 additional minutes to ask—I just have another question or two.

Mr. WHITFIELD. Without objection, I will give you 2 additional minutes.

Mr. MARKEY. I thank the chairman very much.

This is a very serious threat to our country. We know that al Qaeda and others target us and we know that there are many, many PhDs inside of al Qaeda, whether we like it or not. That is what we found in Boston when Mohammad Atta and those other nine were up there in my district plotting on hijacking those tow planes in my district. They were well-educated people, very smart. They tried to find the aperture, and they found out in the aviation system. They are very technically sophisticated people. That is the one thing we did learn about al Qaeda, and that is why I have such a passion for this issue.

Back in 2006, the North American Electric Reliability Corporation proposed some grid security standards that seemed to be fairly limited. One of them even allows utilities to decide for themselves which of their assets are critical and thus subject to the standards in the first place. Only 29 percent of power-generating owners self-reported that they owned a single critical asset. Isn't that right, Mr. McClelland?

Mr. MCCLELLAND. Yes.

Mr. MARKEY. So 70 percent of the electric utility felt they have no critical assets and——

Mr. MCCLELLAND. Critical——

Mr. MARKEY. Excuse me?

Mr. MCCLELLAND. Sorry. I was going to say the distinction is critical cyber assets. Those are the assets that fall under the standards.

Mr. MARKEY. And I just think that that is a mentality here that we have to be realistic about. You know, we have moved to a new era. We are potentially under assault in this sector in the same way that you mentioned, Mr. Chairman, the attack on the Iranian nuclear facility. That was just a very smart way of some very smart people figuring how to disable a nuclear power plant in Iran from a distance, and thank goodness whoever those people are that they were able to do it, disable it and still not cause a nuclear disruption, but there may be others that are not so benign in what their objectives are and the harm that they can do.

So I just think that this isn't something where you self-identify yourself as potentially being a problem. I think we have to decide that there is a problem and that al Qaeda is out there. Do you agree with that, Mr. McClelland?

Mr. MCCLELLAND. Yes, and I would just add one distinction, that NERC has submitted a standard to the commission where critical assets, now, there are several designations for critical assets. Assets that serve nuclear facilities, for instance, are now deemed critical assets. The commission, however, has requested additional information because critical assets are not the assets that are covered by the standard. It is critical cyber assets. So the commission has asked, one of the lines of questions is, tell us how that translates to critical cyber assets because those indeed are still self-determinations.

Mr. MARKEY. Is NERC's guidance advisory or mandatory?

Mr. MCCLELLAND. The standard that NERC has proposed to the commission would be mandatory, and that would be the designation, bright-line designations of critical assets which can help guide an entity to self-determine critical cyber assets, which fall under the standard.

Mr. MARKEY. Thank you. Thank you, Mr. Chairman.

Mr. WHITFIELD. Thank you all. Thank you once again for testifying. We look forward to working with you.

At this time I would like to call up the third panel of witnesses. That would be Mr. Gerry Cauley, President and CEO of North American Electric Reliability Corporation, Mr. Franklin Kramer, former Assistant Secretary of Defense for International Security Affairs at the U.S. Department of Defense, and Mr. Barry Lawson, Associate Director, Power Delivery and Reliability at the National Rural Electric Cooperative Association.

Welcome to the hearing. We look forward to your testimony. At this time, Mr. Cauley, I will recognize you for 5 minutes for the purposes of your opening statement.

STATEMENTS OF GERRY CAULEY, PRESIDENT AND CEO, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; FRANKLIN D. KRAMER, FORMER ASSISTANT SECRETARY OF DEFENSE FOR INTERNATIONAL SECURITY AFFAIRS; AND BARRY R. LAWSON, ASSOCIATE DIRECTOR, POWER DELIVERY AND RELIABILITY, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

STATEMENT OF GERRY CAULEY

Mr. CAULEY. Thank you, and good afternoon, Chairman Whitfield and Ranking Member Rush and members of the subcommittee and fellow panelists.

As CEO of the organization charged with ensuring reliability and security of the North American grid, I wake up every day concerned about emerging risks caused by the intentional actions of our adversaries who would want to harm our Nation and our citizens.

The security of the North American bulk power system is an utmost priority for NERC. The mainstay of NERC's critical infrastructure program is a set of nine cybersecurity standards that we actively monitor and enforce. We have recently made significant strides in improving our cyber standards.

When I came on board at NERC in 2010, I recognized the importance of establishing bright-line criteria, as we just heard from the previous testimony, to identify critical assets to be protected. A new standard was developed in 6 months and filed with the commission in February of this year and is pending their approval. Our standards process works for what it was intended to do: to establish sustained baseline requirements for the reliability and resilience of the bulk power system.

However, there is no single approach, not even compliance with mandatory standards, that will protect the grid against all potential threats from physical and cyber attacks. The threat environment is constantly changing and our defenses must keep pace. Achieving a high degree of resilience requires continuously adapt-

ive measures beyond those outlined in our standards, measures we are actively pursuing today.

The most important of these activities is the operation of our electricity sector information sharing and analysis center. In this role, NERC works closely with Federal partners to promptly disseminate threat indications to electricity sector participants. NERC staff has the necessary security clearances to work with the Department of Homeland Security, DOE and Federal intelligence agencies to generate unclassified recommendations and actions for industry.

Using this process, NERC has issued 14 security-related alerts since January 2010 covering such items as Aurora, Stuxnet, Night Dragon and others. The NERC alert system is working well. Coupled with our CIP standards and the option of using a new expedited and confidential process for developing standards, NERC has a strong foundation of tools we need to protect the cybersecurity of the bulk power system.

As outlined in my written testimony, NERC is leading a number of other initiatives to ensure the resilience of the bulk power system including joint efforts with DOD, DHS and Department of Energy. We are preparing an industry-wide grid exercise in November 2011. Jointly with DOE labs, we are initiating a program to monitor grid cybersecurity of the grid networks and another program to improve the training and qualification of industry cyber experts.

With regard to the proposed draft legislation, first and foremost, NERC has consistently supported legislation to address cyber emergencies and to improve information sharing between government and the private sector. NERC has consistently supported comprehensive legislation authorizing a government entity to address cyber emergencies. Which agency is a policy decision for Congress. NERC stands ready to assist and respond to designated grid security threats.

Measures to improve information sharing between the government and private sector of critical infrastructure are needed. NERC commends the provisions of the discussion draft directing the commission to facilitate sharing of protected information. While the focus on providing adequate security clearances is key, this alone is not enough. It is most important to develop methods for declassifying sensitive information to make it available to industry decision makers. New authority to address grid security vulnerabilities, however, is unnecessary. FERC already has the authority under the Federal Power Act, section 215(d)(5), to direct NERC to prepare a standard to address a specific vulnerability. If Congress decides to allow vulnerabilities to be addressed through a FERC rule or order, at a minimum, the ERO should be given the opportunity to address the identified vulnerability before FERC acts with FERC given a backstop authority if the ERO fails to address the vulnerability within a prescribed period. While we appreciate the language in the current draft which calls for FERC to request and consider our recommendations if time allows, we believe more is needed.

Other provisions of the discussion draft are not needed. NERC has issued information to ensure the industry understands and is mitigating the Aurora vulnerability. The provisions on geomagnetic

storms and spare transformers also are not needed as FERC already has the authority to order us to address these topics today. NERC is actively working on the GMD issue including a recent workshop and an alert providing industry with operational and planning actions to prepare for the effects of a severe geomagnetic disturbance.

In addition, a NERC task force is focused on mitigating risks associated with long lead time transformers and developing a secure database for sharing information on spare equipment.

Finally, the ERO should be given authority under FERC oversight to address grid security vulnerabilities by enforceable means other than standards. Congress has provided us with many tools to address security. As noted previously, we have three levels of alerts. We have strong industry participation and response to these alerts including a provision to authorize NERC subject to FERC oversight to promulgate legally enforceable directives would enhance the security of the power grid. I believe legislation addressing the security of our Nation's electricity infrastructure could be beneficial but the framework should focus on enabling information sharing between government and industry and problem solving between the private and government sectors.

Thank you for the opportunity to speak today, and I look forward to your questioning.

[The prepared statement of Mr. Cauley follows:]

Summary of the Testimony of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation
May 31, 2011

The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk power system. This responsibility encompasses the security of cyber assets essential to the reliable operation of the electric grid. NERC works with government agencies, industry, and consumers to support a coordinated, comprehensive effort to address grid cybersecurity. NERC's FERC-approved critical infrastructure protection (CIP) reliability standards are one of only two sets of mandatory cybersecurity standards in place across the critical infrastructures of the United States today. In addition, NERC's three-level Alert system informs industry and recommends preventative actions to address imminent and non-imminent cyber threats and vulnerabilities. These existing processes should be enhanced, not pre-empted, by grid cybersecurity legislation. NERC has the following recommendations on the draft legislation:

Government authority to deal with cyber emergencies is needed. NERC has consistently supported comprehensive legislation authorizing a government entity to address cyber emergencies. Which agency is a policy decision for Congress to make. Whatever approach is chosen, NERC stands ready to assist in responding to identified grid security threats.

Measures to improve information sharing between the government and private sector owners of critical grid infrastructure are needed. NERC commends the provisions of the discussion draft directing the Commission to facilitate sharing of protected information. While the focus on providing adequate security clearances to key industry personnel also is welcome, this is not enough to assure that actionable information will get to those who need it. It is most important to develop methods for de-classifying sensitive information so that key data can be made available to industry decision-makers.

Additional authority to address grid security vulnerabilities is not necessary. FERC already has authority under FPA Sec. 215(d)(5) to direct NERC to prepare a standard to address a specific vulnerability. Proposed new FPA Section 215A(c) is not needed. If Congress decides to address vulnerabilities through a FERC rule or order, at a minimum, the ERO should be given the opportunity to address the identified vulnerability *before* FERC acts, with FERC given backstop authority to act if the ERO fails to address the vulnerability within a prescribed period.

Other provisions of the discussion draft are not needed. Section 215A(c)(2) is not required as the industry now understands and is mitigating the Aurora vulnerability. The provisions on geomagnetic storms and spare transformers also are not needed, as FERC already has the authority under Sec. 215(d)(5) to order NERC to address these topics.

The ERO should be given authority to address grid security vulnerabilities by enforceable means other than reliability standards. The legislations should include provisions to authorize NERC to promulgate legally enforceable directives in response to the Commission's identification of a grid security vulnerability and a Commission order to NERC to address that vulnerability would enhance the cybersecurity of the grid.

Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation
Before
The Energy and Power Subcommittee of the House Energy and Commerce Committee

Hearing on Discussion Draft Legislation to Improve Cybersecurity of the Electric Grid

May 31, 2011

Introduction

Good morning Chairman Whitfield, Ranking Member Rush, members of the Committee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have more than 30 years' experience in the bulk power system[1] industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program. I appreciate the opportunity to testify today on the discussion draft of electric grid cybersecurity legislation.

NERC's Mission

NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system. NERC is an independent corporation whose membership includes large and small electricity consumers, government representatives, municipalities, cooperatives, independent power producers, investor-owned utilities, independent transmission system operators and federal power marketing agencies such as TVA and

[1] The Bulk Power System (sometimes referred to as "BPS") is defined in Section 215(a)(1) of the Federal Power Act ("FPA") as: "(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."

Bonneville Power Administration. Because the electric grid spans the U.S.-Canada border, NERC's membership includes a number of Canadian entities.

In 2007, NERC was certified as the Electric Reliability Organization (ERO) within the United States by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. Upon approval by FERC, NERC's reliability standards became mandatory within the United States. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by mankind. Throughout North America, four interconnections with a capacity of over one-million megawatts of generation and nearly half-a-million miles of high voltage transmission lines all acting in unison, meet the electric needs of more than 340 million people, with a maximum demand of nearly 850 thousand megawatts. The electricity being used in this room right now is generated and transmitted in real time over a complex series of lines and stations from as far away as Ontario or Tennessee. As

complex as it is, few machines are as robust as the bulk power system. Decades of experience with hurricanes, ice storms and other natural disasters, as well as mechanical breakdowns, vandalism and sabotage, have taught the electric industry how to build strong and reliable networks that generally withstand all but the worst natural and physical disasters while supporting affordable electric service. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electric industry culture of reliability, affecting how it plans, operates and protects the bulk power system.

The Cybersecurity Challenge for the Grid and NERC's Approach to Addressing It

Along with the rest of our economy, the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the reliability of the bulk power system. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the bulk power system requires constant vigilance and expertise.

As CEO of the organization charged with overseeing the reliability and security of the North American grid, I am deeply concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks where we are left to imagine scenarios that might occur and prepare to avoid or mitigate the consequences. Some of those consequences could be much more severe than we have previously experienced. I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from

conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature.

The most effective approach against such adversaries is through thoughtful application of resiliency principles, as outlined in a National Infrastructure Advisory Council (NIAC) report on the grid delivered to the White House in October 2010. I served on that council along with a number of industry CEOs. Resiliency requires proactive readiness for whatever may come our way and includes robustness; the ability to minimize consequences in real-time; the ability to restore essential services; and the ability to adapt and learn. The NIAC's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved sharing of actionable information by government regarding threats and vulnerabilities; 3) cost recovery for security investments driven by national policy; and 4) a strategy on spare equipment with long lead times, such as electric power transformers.

The Administration's recently issued cybersecurity proposals are consistent with these resiliency principles. NERC supports the Administration's comprehensive approach, particularly its emphasis on public-private partnerships and consensus measures to enhance the cybersecurity of all critical infrastructures.

Critical Infrastructure Protection ("CIP") Reliability Standards and other NERC Measures to Address Cybersecurity Threats and Vulnerabilities

1. Reliability Standards

In the Energy Policy Act of 2005, Congress expressly defined the reliability standards to be developed by the ERO and approved by FERC as "including cybersecurity protection …." Sec. 215(a)(3). NERC has nine existing CIP standards that address the following areas:

- Standard CIP-001: Covers Sabotage Reporting.

- Standard CIP-002: Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.
- Standard CIP-003: Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
- Standard CIP-004: Requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
- Standard CIP-005: Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
- Standard CIP-006: Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.
- Standard CIP-007: Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
- Standard CIP-008: Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.
- Standard CIP-009: Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

In December 2010, NERC approved an enhancement to its Critical Cyber Asset Identification standard (CIP-002 version 4) that establishes bright-line criteria for the identification of critical assets. This enhanced standard was filed with FERC in February 2011 and is currently pending FERC approval.

Compliance with the NERC CIP standards is an important threshold for properly securing the BPS. However, there is no single security asset, security technique, security procedure or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best-practices call for additional processes, procedures and technologies beyond those required by the CIP standards.

Since it became the ERO, NERC, working with FERC, has developed mechanisms to promulgate standards on an expedited and/or confidential basis if necessary to address imminent or longer term national security threats. In addition, FERC can order NERC to develop a reliability standard or a modification to a reliability standard to address a specific matter (such as a cyber threat or vulnerability) under FPA Section 215(d)(5).[2] Finally, the NERC Board of Trustees may propose and adopt a standard in response to a FERC directive if the board determines that the regular standards process is not being sufficiently responsive to the Commission.

2. NERC Alerts

Not all vulnerabilities can or should be addressed through a reliability standard. In such cases, NERC Alerts are a key element in critical infrastructure protection. To address cyber

[2] "Section 215(d)(5) of the FPA authorizes the Commission to direct the ERO to submit to the Commission a new or modified Reliability Standard that addresses a specific matter if the Commission considers the new or modified Standard appropriate to carry out section 215." *Order Denying Rehearing, Denying Clarification, Denying Reconsideration, and Denying Request for Stay re North American Electric Reliability Corporation*, 132 FERC ¶ 62,218 (2010).

challenges not covered under the CIP Standards, NERC works through its Electricity Sector-Information Sharing and Analysis Center (ES-ISAC) to inform the industry and recommend preventative actions.

NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies, including the Department of Homeland Security and the Department of Energy National Laboratories, and bulk power system subject matter experts, called the HYDRA team, to communicate sensitive information to the industry. As defined in NERC's Rules of Procedure, the ES-ISAC developed the following three levels of Alerts for formal notice to industry regarding security issues:

- **Industry Advisory** - Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- **Recommendation to Industry** - Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the Alert.
- **Essential Action** - Identifies actions deemed to be "essential" to bulk power system reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the Alert.

The risk to the bulk power system determines selection of the appropriate Alert notification level. Generally, NERC distributes Alerts broadly to some 1900 users, owners, and operators of the bulk power system in North America, utilizing its Compliance Registry. NERC also distributes Alerts to other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g.; Balancing Authorities, Planning Authorities, Generation Owners, etc.).

NERC has issued 14 CIP-related Alerts since January 2010 (12 Industry Advisories and two Recommendations to Industry). Those Alerts covered items such as Aurora, Stuxnet, Night Dragon and the reporting of suspicious activity. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders. In addition, NERC released one Joint Product CIP Awareness Bulletin in collaboration with DOE, DHS and the FBI titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)".

The NERC Alert system is working well. It is known by industry, handles confidential information and does so in an expedited manner. An Alert does not require a NERC balloting process, but it is not enforceable as reliability standards are.

NERC Works with DOD, DHS and DOE to Protect Grid Cybersecurity

As chair of the Electricity Sub-Sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the government, including the Department of Defense, the Department of Homeland Security and the Department of Energy, to discuss and identify critical infrastructure protection concepts, processes and resources, as well as to facilitate information sharing about cyber vulnerabilities and threats. This type of public/private partnership is key to effective cybersecurity protection.

Recently, I met with officials from U.S. NORTHCOM where we discussed collaborating on various electric grid-focused activities including participation in the 2011 SecureGrid Exercise, providing electric sector situational awareness and collaborating on the Joint Capability Technology Demonstration (JCTD) Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). The latter project is being proposed to

understand how specific facilities could develop small reliable "micro-grids" on a short-term or emergency basis.

NERC is working with DHS National Cybersecurity and Communications Integration Center to develop a Memorandum of Understanding for bi-directional sharing of critical infrastructure protection information between the government and the electricity sector in North America. NERC also provides leadership to two significant DHS-affiliated public-private partnerships. These are the Partnership for Critical Infrastructure Security (PCIS) and the Industrial Control Systems Joint Working Group (ICSJWG). The PCIS is the senior-most policy coordination group between public and private sector organizations. On the government side, PCIS comprises the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating Councils. On the private side, PCIS comprises the chairs of all of the private-sector coordinating councils. The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC is engaged with DOE National Laboratories to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the bulk power system. We are working with Pacific Northwest National Laboratory on the Electric Sector Network Monitoring initiative and also on developing cybersecurity certification guidelines for Smart-Grid Cyber Operators. In a similar fashion, NERC is working with the Idaho National Laboratory to promote the Cyber Security Evaluation Tool for use within the electric sector. NERC also is

partnering with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability and security incident information.

Finally, NERC is working with DOE and the National Institute of Standards and Technology to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including both the bulk power system and distribution systems. We believe this to be particularly important with the increasing availability of smart-grid and smart-meter technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the bulk power system. Everyone engaged in smart-grid and smart-meter implementation should ensure that appropriate security applications and technologies are built into the system to prevent the creation of additional threats and vulnerabilities.

NERC Comments on the Discussion Draft

1. **Government authority to deal with cyber emergencies is needed.**

NERC has consistently supported comprehensive legislation authorizing some government entity to address cyber emergencies. Which agency is a policy decision for Congress to make; the current draft would give the Commission that authority, upon a determination by the President identifying an imminent grid security threat. Whatever approach is chosen, NERC stands ready to assist in responding to identified grid security threats.

2. **Measures to improve information sharing between the government and private sector owners of critical grid infrastructure are also needed.**

NERC strongly supports efforts to improve information sharing between government and the private sector owners of critical electric infrastructure. NERC especially commends the provisions of the discussion draft directing the Commission to facilitate the appropriate sharing

of protected information between and among government entities and those in the private sector who are subject to the proposed legislation.

NERC and the electric industry can only deal with the risks they are aware of. It is impractical, inefficient and impossible to defend against all possible threats or vulnerabilities. Entities must prioritize their resources to protect against those risks that pose the greatest harm to their assets and their customers. The electric industry best understands the impact that a particular event or incident could have on the bulk power system, but the industry does not have the same access to actionable intelligence and analysis that the government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and vulnerabilities. Too often the industry has heard from government agencies that the threats are real, but is given little or no additional information. This leads to frustration among the private sector entities that are unable to respond effectively due to ill-defined and nebulous threat information.

NERC appreciates the attention in the discussion draft to providing adequate security clearances to key industry personnel, but this alone cannot effectively address the unavailability of actionable information for electricity industry decision-makers. NERC has over 1900 entities on its Compliance Registry; some have just a few employees and some have many thousands. Given the necessarily limited number of security clearances that may be made available, it is more important to develop methods for declassifying sensitive information so that key data can be made available to the broad range of industry decision-makers who must act to protect the grid against the threat or vulnerability.

3. Additional authority to address Grid Security Vulnerabilities is not necessary.

As discussed above, NERC has the existing tools, the expertise and the relationships with government agencies, intelligence resources and industry subject matter experts to address identified vulnerabilities effectively and efficiently. In addition, FERC has the authority under FPA Sec. 215(d)(5) to direct NERC to prepare a standard to address a specific vulnerability or other matter, and to do so by a certain date, if FERC decides the matter needs that level of priority. Thus, it is not clear to NERC that the vulnerability section (proposed new FPA Section 215A(c)) is needed.

If Congress decides to address vulnerabilities through a FERC order, at a minimum, the ERO should be given the opportunity to address the vulnerability identified by FERC within a time certain, , similar to the current authority under Sec. 215(d)(5).

With respect to the existing cybersecurity vulnerability addressed in proposed Section 215A(c)(2) of the discussion draft, the industry now understands the Aurora vulnerability and is mitigating that vulnerability. Therefore, NERC believes section 215A(c)(2) is not needed. From 2007 through 2010, NERC worked closely with federal partners on information controls and was finally authorized to share with industry an extensive technical library through NERC's protected portals. The availability of this technical library allowed NERC, federal partners, and industry subject matter experts to develop and issue an Aurora "Recommendation to Industry" Alert on October 13, 2010 with explicit information on the vulnerability and recommendations for detailed mitigation measures. More importantly, the availability of the technical library allowed the asset owners to assess for themselves the true nature of the Aurora vulnerability and begin to devise mitigations to address that vulnerability. This NERC Level 2 "Recommendation to Industry" carried mandatory reporting obligations in accordance with NERC Rules of Procedure

(ROP)[3] and NERC continues to work with industry on mitigation efforts. Over the past three weeks, NERC has held Aurora mitigation webinars attended by over 800 industry subject matter experts.

4. ERO Authority to Address Grid Security Vulnerabilities by enforceable means other than Reliability Standards would be useful.

Not all Grid Security Vulnerabilities can or should be addressed by a reliability standard. Currently, however, NERC actions other than reliability standards are not legally enforceable. Legislation authorizing NERC to promulgate legally enforceable directives in response to the Commission's identification of a Grid Security Vulnerability and a Commission order to NERC to address that vulnerability could enhance the cybersecurity of the grid. In order to be enforceable, such an ERO directive would need to be approved by the Commission.

5. Geomagnetic Storms and Spare Transformer provisions are not needed.

Section 215A(c)(4) and (c)(5) of the discussion draft address, respectively, geomagnetic storms and large transformers. NERC is currently working with two separate task forces to address geomagnetic storms and spare transformer issues. NERC's Geomagnetic Disturbance ("GMD") Task Force recently held a workshop focused on potential mitigation approaches and issued an Industry Advisory NERC Alert on GMD.[4] This Alert provides industry with guidance to prepare for the effects of severe GMD on the bulk power system.

With respect to spare transformers, in September 2010, NERC initiated the Spare Equipment Database (SED) Task Force to redesign and update the policies and protocols for the use of this Database across North America. This effort is also designed to obtain broader participation by bulk power system owners and expanded information on spare transformers. In conjunction with EEI's Spare Transformer Equipment Program, and the many pooling/bilateral

[3] Section 810, *Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions.*
[4] http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01_GMD_FINAL.pdf.

agreements that exist today among industry participants, NERC's SED program will support utilities in responding to and managing bulk power system reliability in the event of an event that causes loss of transformers.

Currently, FERC can order NERC to address either one of these topics under Sec. 215(d)(5). Consequently, these legislative provisions in the discussion draft are not needed. If Congress chooses to direct action on these topics as a high priority, however, NERC supports the language in the discussion draft that requires FERC to specify the nature and magnitude of the reasonably foreseeable events or attacks against which reliability standards must protect (in the case of geomagnetic storms) or which provide the basis of the standards (in the case of large transformer availability). NERC also supports the provisions in the discussion draft requiring that such standards appropriately balance the risks associated with a reasonably foreseeable attack or event, including any regional variation in such risks, with the costs of mitigating such risks.

Conclusion

NERC works with multiple agencies, industry, consumers and government to support a coordinated comprehensive effort to address cybersecurity. As outlined today, NERC has many tools available including the ESCC and the ES-ISAC to address imminent and non-imminent threats and vulnerabilities through its Alerts and reliability standards processes in a timely, efficient and effective manner. These existing processes should be enhanced, not pre-empted, by cybersecurity grid legislation.

We appreciate this opportunity to discuss NERC's activities on cybersecurity with the subcommittee and to offer our views on legislation that would improve cybersecurity protection of the grid.

Mr. WHITFIELD. Thank you, Mr. Cauley.

Mr. Kramer, you are recognized for 5 minutes for an opening statement.

STATEMENT OF FRANKLIN D. KRAMER

Mr. KRAMER. Thank you, Mr. Chairman and Mr. Ranking Member, Mr. Terry. I appreciate the opportunity to testify.

I think the proposed legislation, the GRID Act that you have the discussion draft, is excellent but I would like to suggest five things that would actually make it better, at least from my perspective.

The first is I think that we need mandatory Federal standards. We need to turn the system around and have the Federal agency, be it FERC or, as in the administration's discussion draft, DHS have the authority to issue standards.

Secondly, I think that we need to focus much more on the issue of resilience, how will we deal with the problem of how the grid will operate in the face of attack.

Third, I think that all elements of the Federal Government and including especially the DOD have to be given clear authority to help protect and/or respond to an attack on the grid because it is only the DOD that has the capabilities that are necessary.

Fourth, I think we have to think about the issue of scale and resources and particularly the issue of cost and make sure that the industry can recover its costs.

And lastly, I think there needs to be a much more extensive research and development program to deal with the advanced threats. We need advanced capabilities.

The reason I say that, Mr. Chairman, all these points, is what you have already said. The threat is increasing. We have seen, for example, last year an attack on Google. We have seen more recently an attack on a company called RSA, very advanced cyber companies, and as you mentioned, we have seen the Stuxnet attack. Those control systems that were attacked in Stuxnet are precisely the kind of control systems that control the electric grid. The vulnerability is very, very substantial, and has been pointed out by others already in this hearing, right now with the smart grid increasingly coming into play, the distribution system as well as the generation system, the transmission system are sources of vulnerability, so I think we really need to focus on the entirety of the problem and recognize how much the threat has been increasing over time.

The reason I say that we need mandatory standards is that frankly the current system is just too slow. It doesn't work quickly. It hasn't satisfied the problem. In fact, if you look at NERC's own, I think it was called high-impact, low-frequently study last year, it said very clearly that the grid is at risk against an advertent adversary. If we think about other areas—clean air, clean water, automobile safety standards—the Federal Government issues the standards. It certainly allows industry to comment, but I think that is the way we ought to do it.

In addition, I think that the current act, the discussion draft, has what is called authority for the FERC if there was a so-called imminent threat. But I think that imminent is too late often. What we really need is if we see a significant threat where one needs to

be able to take prompt action before we get to that microsecond before the attack occurs. The Federal Government ought to have that authority so it can issue interim standards but earlier than the imminent-threat standard.

On the resilience point, I think we all know—and again, if you look at the Google attack or Stuxnet or the like, is that cyber offense beats cyber defense. In fact, the Deputy Secretary of Defense has said that publicly and plenty of others have. In the DOD area, the DOD doesn't just rely on passive defense, it also does what is called active defense, and if DOD needs to do active defense to protect its network's critical infrastructure, and again, we have heard and I have said myself and others said today the DOD relies 99.9 percent on commercial electricity. Well, that means that commercial electricity ought to have the same kind of protection, that active defense. I don't think that the industry should do it, I think the DOD under the right kind of standards, legislative standards, regulations, guidance from the President, ought to work with the sector-specific agency and also with the industry to be able to provide that.

We also need to have capabilities that we haven't heard talked about today. We need what I call gold standard integrity: integrity of data, integrity of software, integrity of hardware. We need capabilities like segmentation and isolation so that the key elements of the grid can be protected by being separated from other elements of the grid.

We want to look also finally at the issue of scale and resources. It is a very large enterprise. We are going to have to have the private sector work to get it out there. It seems to me that if the industry is going to incur cost, and this is a highly regulated industry, that it ought to be able to recover those costs. That could be done directly or indirectly with the Federal Government. It could be in the rate base. But it should be allowed in some way, shape or form.

And finally, as I said, I think we need to have a comprehensive R&D program so that when we have advanced threats, we can have advanced capabilities to meet them.

And with that, Mr. Chairman, I appreciate the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Kramer follows:]

Statement of Franklin D. Kramer
before the
House Energy and Commerce Committee
Subcommittee on Energy and Power
May 31, 2011

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify on the subject of cyber security and the electric grid. I am appearing today solely in my individual capacity, and my testimony is only my own.

To summarize, my key points are: the need for mandatory government-generated standards since the current approach is insufficient; the importance of being able to generate resilience of the electric grid in the face of attack; the need to use all the capabilities of the federal government to protect the grid, including those of the Department of Defense and the intelligence community working in conjunction with the agency responsible for electric grid security and with the private sector; the requirements of scale and resources; and the need to include the distribution system under an effective cyber security approach for the electric grid.

The testimony which follows is divided into three parts:
--the threats to and vulnerabilities of the electric grid, and the national security implications potentially resulting from an attack on the grid;
--the requirements of an effective cyber security approach for the electric grid; and
--the extent to which the GRID Act and other proposed legislation meet or could be improved to meet those requirements.

1. Threats, Vulnerabilities and National Security Implications. The electric grid's vulnerability has been well-documented on numerous occasions, including hearings before this Committee, statements by the President of the United States, and numerous governmental and other studies. The electric grid has become substantially dependent on cyber capabilities over the past 15 years, and the well-known attacks on Google, RSA, and Comodo—three very highly capable information technology companies--as well as the STUXNET and WikiLeaks incidents, underscore the vulnerability of cyber infrastructures—vulnerabilities which are all shared by the electric grid.

From a technological point of view, these vulnerabilities raise issues of remote attack (with multiple vectors); close-in attack; insider attack; and possibly in the broader Iranian nuclear context, supply chain attack. All involve critical technical vulnerabilities and exploits.

From a policy point of view, they raise the issues of protection, prevention, and resilience—and the questions of scale, resources, and governance necessary to accomplish those tasks.

The importance of recognizing this vulnerability cannot be overstated. The vulnerabilities exist despite the existence of cyber security standards for the electric grid which have been promulgated under Section 215 of the Federal Power Act.

The North American Electric Reliability Council's High Impact, Low Frequency study issued in June 2010 stated "the bulk power system remains an attractive target for acts of both physical and cyber terrorism," and further concluded:

"A highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes. . . . . [A] coordinated attack would involve an intelligent adversary with the capability to quickly bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods."[1]

The impact would be very significant, both from a national security and an economic perspective. As I have noted in prior writing: "There is an important additional reason why the grid deserves high level attention: the DOD cannot function without electricity. While there is considerable focus in the DOD at this time on that vulnerability, and many efforts toward off-grid power solutions, very significant vulnerability currently exists and will continue to exist for a long time. Further, even if the DOD made its own facilities relatively immune to grid disruption, the Pentagon depends heavily on other civilian

[1] NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, at p. 26.

infrastructures that themselves rely on electricity, the most obvious being telecommunications, but also all elements of transportation and logistics."[2]

What is true of the Department of Defense is true of virtually all governmental, private sector and individual functions in the United States. As an advanced technological nation, we run on electricity.

During the past year, we have had even further confirmation of the problem of the grid's vulnerability, as demonstrated by the STUXNET attacks. STUXNET—while not grid-directed, showed the vulnerability of control machines—which are the very type of machines upon which the grid depends for effective operation. STUXNET has been publicly analyzed in numerous places, and the Committee will be fully familiar with its implications. STUXNET shows also that not only are the offense and defense at play in the cyber arena—but if one accepts numerous public accounts (such as set forth in the New York Times and many other places) that the offense is well ahead of the defense.

Finally, one important ongoing change for the grid is the expected emergence of the smart grid. The smart grid has multiple aspects, but a key element will be the connectivity between the consumer, supplied by the distribution system, and the generation/transmission portions of the grid. Such connectivity means that the distribution system could be a key vector for a national security attack on the grid. That is a newly significant issue, and one which deserves this Committee's consideration.

In sum, the vulnerability of the electric grid is a critical national security problem. Failure to resolve it could have devastating national security and economic consequences.

2. Requirements of Effective Cyber Security for the Electric Grid. Effective cyber security for the electric grid will have three key elements, including A) key cyber security capabilities, B) appropriate cyber security governance directed to the roles and responsibilities of the federal government and the private sector, and C) continuing efforts on research and development to generate currently needed capabilities and meet future threats.

A. Capabilities. The requirements of cyber security for the grid include:

[2] Kramer, Cyber Security: An Integrated Governmental Strategy for Progress, at p. 8 (2010).

--First, the problem of protecting interlocking multiple, including some very large, enterprises—there are some 3200 power generation companies in the North American grid. Thus, the problems of scale and the resources necessary to act are critical to consider.

--Second, the issue of appropriate technologies and processes, including the necessity of trained personnel. There currently is no agreed architectural approach that companies can use to provide adequate cyber security—that is why current vulnerabilities exist, and why existing standards are not sufficient. And there are insufficient trained cyber security experts.

--Third, the need to be able to operate despite attack. All believe that under current conditions, cyber offense beats cyber defense, so the question is, expecting to have cyber defenses penetrated, how to keep the appropriate elements of the grid effectively operating. The most important requirement of cyber security for the electric grid will be its resilience under attack.

The cyber security requirements challenge, therefore, is to develop:
1) an overall approach including technologies and processes,
2) courses of action that, based on the technologies and processes, provide resilience, and
3) the people capable of doing this.

It is also important to recognize that successful cyber security likely will involve a strategic framework that goes beyond defense and resilience. In protecting Department of Defense networks, the DOD is also focused not only on passive defense, but also on "active defense" and "offensive" cyber. "Active defense" means using sensors and capabilities at the perimeter of the DOD enterprise to affect the attacker. "Offense" means using cyber as one would any other DOD capability—kinetic or electronic warfare, for example. It certainly is not the case that any private enterprise without government involvement could or should undertake active defense or offensive action, as the DOD has prepared for (although, of course, private entities can protect their own networks, technology and information with appropriate measures[3]). However, if DOD networks require this type protection, it would appear that such protection would be important to the electric grid were it under attack.

[3] One important legislative question is to what extent and under what circumstances, including possibly government authorization, should Internet Service Providers undertake protection from the network for their customers.

Accordingly, it would seem appropriate for the DOD with the right legislative authority and under Presidential guidance to help protect electric grid networks. To paraphrase the substance of what one electric power company official said to me (and this is a paraphrase), "I can understand why my company should be able to protect itself against cyber criminals, but why should I be expected to succeed against a major nation state cyber attack? Isn't that what the government is supposed to do?" That seems to me to be a critical point—a major nation state attack (or a major attack by a terrorist organization) will be different in character and consequence from an attack by criminals against an enterprise. Accordingly, given the consequences of such an attack, I believe legislation should clearly authorize the DOD and the intelligence community, under appropriate guidelines and working with the agency responsible for electric grid cyber protection and with the private sector, to take both anticipatory and responsive steps to protect the grid and to ensure its resilience if it were under such attack.

B. Governance. Inasmuch as the vulnerability of the electric grid presents a national security vulnerability of high consequence, there is, as this Committee's proposed Grid Act indicates, an extremely strong case for new legislation and regulation that would set forth a fully integrated framework to deal with this problem. The current legislative and regulatory governance approach, though it has accomplished some things, has not been sufficiently effective. Just as strong safety requirements for cars and environmental requirements limiting water and air pollution have greatly improved the national posture, legislation and regulation that created an effective requirement for much stronger cyber security for critical infrastructure like the electric grid would meet an important national need. While there is a compelling need for new legislation and regulation, three important considerations need to be taken into account.

First, since the grid is very largely in private hands, but the government has critical capabilities, there needs to be an effective public-private working relationship. However, the current Section 215 process has not provided the degree of cyber security that is adequate. Accordingly, rather than an approach that relies on industry to generate cyber security standards, the federal government should have the responsibility to do so. Generally, the government should act after consultation with industry. However, if there is a significant threat that prompt government action would mitigate, government action should be authorized. That approach is different from the imminent threat standard in the proposed Grid Act. Enhancing cyber security often will be best

accomplished by taking steps well in advance of an imminent threat—for example, in response to reconnaissance by an adversary or otherwise early in the threat cycle, and it may be invaluable not to have to wait for a full-blown regulatory process.

Second, enhancing cyber security may require costs of some consequence to the industry. Legislation should take account of that fact, and that the industry operates under regulatory constraints. Focus on cost recovery would be especially appropriate if industry were required to act where prompt action was required based on a federal decision. But it should also be true when requirements are imposed more generally for national security and national economic purposes. Since cyber security is so critical to the nation, the industry should be able to recover its costs—which could come about through direct or indirect cost recovery from the federal government or through a rate base approach.

Third, the cyber sector has had a very quickly changing nature. Cyber looks very different today than it looked only ten years ago, and there are good reasons to believe that it will significantly change again in ten years. Any regulatory scheme that is not flexible enough to take account of such changes is likely to be far less effective than necessary.

C. Research and Development. As the Google matter and other well-known intrusions show, even very capable companies with extensively deployed cyber security measures are vulnerable. Current capabilities can only go so far. It is generally agreed that an advanced attacker will be able to negate currently available defenses.

The fundamental question that this issue raises, therefore, is whether an enhanced cyber security capability can be created. Or, to put it another way, how valuable would a significant R&D program be? And most specifically, in the context of this hearing, what does that mean for the electric grid? Could, for example, the grid's network nature and topology be taken advantage of to provide resilience in a way that might not be available to a more point type target such as an enterprise or cloud or individual? If it would seem to be valuable, how should such R&D be undertaken, including what should the division of labor be between government and the private sector (including how the government should appropriately leverage private investment)?

There are, of course, many existing R&D efforts. The Department of Energy, particularly through the DOE laboratories, has undertaken excellent research focused on the grid. Many cyber security issues overlap in multiple arenas beyond the grid, and important efforts exist under DOD and intelligence community auspices, including efforts by the Defense Advanced Research Projects Agency (DARPA). Others are at the Department of Homeland Security, which has developed a cyber security R&D program, and at the National Academy of Sciences. There are also substantial resources from the private sector, some in response to the government programs and some independent R&D.

A much enhanced R&D program, including increased efforts focused on the electric grid, nonetheless would be highly valuable to improve cyber security. Such a program could likely profitably be divided among the government (which could do more pure research than in the private sector, could focus on particular types of applications and could help guide private research) and the private and academic sectors (which could benefit from increased government support, but which also will undertake research on their own in order to meet market demands). The key considerations are to have an integrated view of federal cyber security R&D and to ensure that appropriate amounts are being spent on developing particular solutions. Substantively, such an R&D program should have three parts:

• The first would focus on protection – can advanced techniques such as dynamic addressing and moving targets; and segmentation/tailored trustworthy spaces be developed to create much enhanced cyber security.

• The second would assume, as seems entirely likely, that security will not be perfect and will therefore focus on resilience – how to operate a system effectively even though security has been breached. What, for example, would be necessary to implement gold standard integrity for data, software and hardware; how might redundancy or diversity be used to support resilience?

• A third key element would be to develop a systematic approach to measuring security. One element of this would be to greatly enhance the area of modeling and simulations to test the results of both attacks and defenses.

In addition to specific R&D approaches, one important, long-term approach to enhanced R&D would be to greatly expand education and training for cyber

professionals. A significantly increased governmental education/ scholarship program would be very valuable.

3. The GRID Act and Other Proposed Legislation. As the foregoing suggests, the proposed Grid Act and other currently proposed legislation would be substantial improvements on the existing legislation. Focusing on the Grid Act and without reviewing each element of the other legislative proposals, the following recommendations would significantly improve suggested legislation.

A) Legislation should give the government mandatory regulatory authority over the grid, and should eliminate the approach whereby the government (now FERC) only has authority to review reliability standards recommended by the North American Electric Reliability Council. That approach has not provided adequate security and is far too slow in a context of a highly dynamic and dangerous threat environment.

B) Reliability standards should include authorization to require specific technological approaches and processes, as well as personnel requirements. Specific focus should be put on the requirements of resilience since the expectation must be of a breakdown in security—and the need will exist to maintain an adequate level of electric power operations even when the grid is under attack. That may mean that the standards will be significantly higher and that there could be significantly greater requirements for parts of the grid than for others (and advanced capabilities may be particularly important for these parts of the grid). Performance standards are a desirable longer term goal, but until greater R&D has been accomplished, performance standards are unlikely to be feasible for the most part.

C) The Department of Defense and the intelligence community should be legislatively authorized to work with the agency responsible for electric grid security and with the private sector to provide under appropriate guidance anticipatory and responsive actions (to achieve protection, prevention and resilience).

D) The interconnectivity of the grid and its very large scale means that getting effective cyber security capabilities out to the full grid and the resources necessary to do so are highly important. An evaluation/certification process probably will be valuable, although, to be effective, reliability standards will have to be issued against which evaluation/certification can be undertaken. Additionally, since companies whose rates are often regulated are being asked

to work with the federal government to help resolve a national security problem, there should be a mechanism for costs to be recovered. That could be directly or indirectly with the federal government or under a rate base approach.

E) The emergence of the smart grid means that the distribution system can be an important vector for a cyber attack. Cyber security legislation and regulation therefore needs to include the distribution system if effective electric grid security is to be achieved.

F) An expanded R&D program should be undertaken in order that advanced capabilities to meet the dynamic and changing threat can be achieved.

Finally, any efforts by this Committee should, of course, be coordinated with the other committees proposing legislation, both in the House and in the Senate.

* * * * *

I thank you very much for the opportunity to testify, and look forward to your questions.

Mr. WHITFIELD. Thank you.

Mr. Lawson, you are recognized for 5 minutes.

STATEMENT OF BARRY R. LAWSON

Mr. LAWSON. Chairman Whitfield, Ranking Member Rush and members of the subcommittee, thank you for the opportunity to testify today on cybersecurity and the GRID Act. My name is Barry Lawson, and I am the Associate Director of Power Delivery and Reliability at the National Rural Electric Cooperative Association, which represents over 900 member-owned not-for-profit cooperatives providing electricity to 42 million consumers in 47 States.

Over the last decade, I have been involved in a variety of critical infrastructure protection and cybersecurity initiatives with industry, NERC, DHS and DOE. Based on these experiences, I know the electric power industry takes these issues very seriously. Additionally, to my knowledge, there has not been a documented case of a successful attempt to damage the North American bulk power system through cyber means.

While my testimony today is offered on behalf of electric cooperatives, I want to also recognize the longstanding partnership among all sectors of the electric power industry when it comes to reliability and cybersecurity. NRECA is part of a coalition which includes major trade associations representing the full scope of the electric power industry as well as state regulators, large industrial consumers and Canadian utilities. It is rare that we all agree on public policy issues but we unanimously support the NERC process and narrow new authority for the Federal Government in the event of severe, imminent cyber threats.

Under section 215 of the Federal Power Act, NERC works closely with electric power industry experts and others to draft mandatory and enforceable reliability and cybersecurity standards that apply across the North American grid. The standards process can be lengthy when addressing highly technical issues but it can also be shortened when needed using NERC's expedited standards procedures as approved by FERC. NERC also has a FERC-approved process for developing standards in a confidential manner when national security requires it.

NERC rules and procedures also give NERC authority to distribute alerts on topics that are important for industry to address. FERC reviews these alerts before they are released. There are three levels of alerts, and the top two levels have mandatory reporting requirements that typically require recipients to inform NERC what they did in response to the alert. The alert process has quickly and effectively provided industry critical information on many issues including Stuxnet, Night Dragon and geomagnetic disturbances. NERC is required to provide reports to FERC on the top two levels of alerts, explaining the level of action industry has taken. To date, these reports have shown that industry takes these alerts very seriously.

The industry recognizes the threat environment is complicated and that imminent, severe threats are possible. In some cases, even NERC procedures and standards cannot assure that industry gets timely, actionable information to mitigate a threat against the bulk power system. When the Federal Government at the highest levels

determines that emergency action is necessary, it should be able to issue orders to our industry that directly address the severe and imminent cyber threat and set out the mitigation actions needed to protect the bulk power system. Those orders should sunset when the threat has subsided or is mitigated, for example, by development of a related NERC standard.

Our primary concern is that the draft GRID Act creates new authority for FERC concerning vulnerabilities that largely duplicates existing FERC authority and ongoing NERC activities under section 215 and could substantially undermine the existing reliability standards regime. It should be understood that vulnerabilities alone do not adversely impact the reliability of the grid. That being said, our industry has every incentive ranging from financial considerations to the fundamental obligation to serve our customers with reliable and affordable power to protect the grid when vulnerabilities emerge.

The draft GRID Act authorizes FERC if it determines there is a grid security vulnerability that existing NERC standards do not address to issue a rule or order requiring industry to implement measures to protect against the vulnerability. The new authority the draft seeks to give FERC is very concerning to our industry. First, we question whether FERC has the intelligence-handling expertise to exercise such broad new authority. Second, this new authority regarding vulnerabilities would fundamentally alter section 215 by providing FERC an unnecessary role in addressing vulnerabilities that NERC and industry are managing very well through standards and alerts.

To help industry to protect the grid from vulnerabilities and threats, we need timely, actionable intelligence from government. More industry trusted experts need higher levels of security clearances so we can plan effective responses to threats and vulnerabilities. The draft seeks to make improvement in these areas, and we appreciate the subcommittee's support.

In conclusion, we urge the subcommittee to focus on the immediate, narrow issues at hand, the need for very quick emergency orders if the bulk power system faces an imminent cyber attack and the need for the electric power industry to receive timely, actionable information.

Thank you for the opportunity to testify today and I look forward to your questions.

[The prepared statement of Mr. Lawson follows:]

Statement of the National Rural Electric Cooperative Association
to the United States House of Representatives

Committee on Energy and Commerce

Energy and Power Subcommittee

"Protecting the Electric Grid: The Grid Reliability and Infrastructure Defense Act."

May 31, 2011

4301 Wilson Boulevard
Arlington VA 22203
www.nreca.coop

Executive Summary

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 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 and its members have also been very engaged in the development of NERC's reliability standards, including the cybersecurity standards.

The self-regulatory model recognizes the expertise that resides throughout the electric power industry and is the best means of maintaining a strong, reliable bulk power system. Each day, the electric power industry overcomes some level of threat, ranging from those posed by inclement weather or other natural events, to vandalism, equipment failures and cyber events. The NERC reliability standards support industry's capacity to respond to a wide variety of intentional events and natural disasters.

For the overwhelming majority of identified threats, existing industry and NERC procedures, standards and alerts support the necessary response from industry for the continued reliability of the bulk power system. However, with increasing reliance on computerized and telecommunications-enabled controls in electricity infrastructure, some threats may be so severe and imminent that the self-regulatory model - without the benefit of classified intelligence - may not be able to respond as quickly as needed to sufficiently protect the bulk power system. In those limited circumstances, it is appropriate to provide a back-stop, federal emergency authority which extends until the

threat is mitigated, ends or until NERC can adequately address the threat through standards and/or alerts.

Existing industry and NERC procedures, standards and alerts support the necessary response from industry for vulnerabilities. These capabilities and the private-public partnership will be improved as the federal government provides more timely and actionable information and intelligence to the electric power industry.

Introduction

Chairman Whitfield, Ranking Member Rush and members of the Subcommittee, thank you for the opportunity to testify today on cyber-security threats and vulnerabilities, their potential impacts on the bulk power system, and the draft legislation known as the "GRID Act."

My name is Barry Lawson, and I am the Associate Director, Power Delivery and Reliability 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 over 900 cooperatives providing electricity to 42 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.

While my testimony today is offered on behalf of electric cooperatives, I want to also recognize the long-standing partnership among all sectors of the electric power

industry when it comes to reliability and cybersecurity. NRECA is part of an industry wide coalition which includes several major trade associations representing the full scope of electric generation, transmission and distribution in the United States, as well as state regulators, Canadian interests and large industrial consumers. Participating in the coalition are: 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, the Transmission Access Policy Study Group, and the Utilities Telecom Council. Rarely do all of these groups find consensus on public policy issues, but among us, there is unanimous support for ensuring that the public and private sectors can continue to work together effectively to maintain and improve cyber and grid security. My testimony focuses on the value of this cooperative relationship, the unique nature of threats and vulnerabilities facing to the power grid, and the ongoing efforts of the nation's electric sector to respond to threats and vulnerabilities.

Along with many colleagues, including some on the panel today, I work on reliability and cyber and grid security issues with electric cooperatives, other electricity industry sectors, FERC and NERC. From 2008 to the end of 2011, on behalf of NRECA and its members, I chair 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 at NRECA and my role on the CIPC requires me to interact with NERC, the Department of Energy (DOE) and the Department of Homeland Security (DHS) on an ongoing basis

and contributes to the viewpoints I will share with you today. In addition, I am an active member of the Electric Sector Coordinating Council – the ESCC -- which interacts with our sector specific agency – DOE – and other federal government agencies and critical infrastructures on the policy level issues related to critical infrastructure protection. Mr. Cauley from NERC is the Chair of the ESCC. For the last decade, I have been involved in critical infrastructure protection issues, including those related to cyber security. I can tell you based on my own experience that the electric power industry takes cyber threats and vulnerabilities very seriously. However, to my knowledge, including that gained serving in various leadership roles, there are no documented cases of successful attempts to damage the North American bulk power system through cyber channels.

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, transmission and distribution 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.

Existing NERC Procedures Guide Industry through Threats and Vulnerabilities

Congress approved a mandatory and enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005, known as Section 215. Under Section 215 NERC works closely with electric power industry experts, regional entities, FERC staff and other government representatives, to draft mandatory and enforceable

reliability and cyber security standards that apply across the North American grid, including Canada and parts of Mexico. Electrons don't recognize borders.

FERC has the authority to then approve or remand those standards as they apply in the United States. The Canadian provinces have voluntarily entered into MOUs with NERC to determine how they will address compliance with the approved standards. NERC and FERC can levy fines on U.S. entities that violate the standards and have done so. Additionally, FERC can direct NERC to develop new or revised reliability standards within a specific timeframe. The reliability standards cover physical **and** cyber aspects of the grid. Therefore, NERC today 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.

The standards process can sometimes be lengthy to accommodate the highly technical nature of the subject matter, but it can also be shortened when needed. The NERC Standards Process Manual, as approved by FERC, provides for an expedited standards development process that can significantly shorten the standards development timeline. Additionally, NERC also has a process for developing standards in a confidential manner, in response to and in consideration of, national security and emergency issues.

The NERC Rules of Procedure also provide NERC with the authority to distribute alerts on topics that are important for industry to address. FERC reviews these alerts but they are distributed by NERC. There are three levels of alerts: Advisory, Recommended Action and - the most critical advisory level - Essential Action. Recommended Action

and Essential Action Alerts have mandatory reporting requirements that typically demonstrate what action an entity has taken. We strongly support NERC's use of the alert tools to quickly – within hours or days – distribute important information to the industry for action. In fact, NERC and the industry have used the alert process successfully to distribute critical information related to many issues, including Stuxnet, Night Dragon, geomagnetic disturbances and many other cyber and operational issues. NERC is required to provide reports to FERC on Recommended and Essential Action alerts explaining the level of action industry has taken. To date, those reports have shown that industry takes these alerts seriously by demonstrating the high level of industry response to the issues identified in the alerts.

Viewpoints on "GRID Act" Discussion Draft

NRECA, working closely with its counterparts across the electric industry, agrees there is potential for some threats so imminent and severe that even the comprehensive, carefully designed NERC procedures and standards 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, the federal government should have the authority to issue orders (after coordination with the industry and relevant governmental authorities in Canada and Mexico) that directly address the threat and the necessary mitigation actions needed to protect the bulk power system.

Our over-arching concern is that the draft GRID Act creates new authority for FERC concerning vulnerabilities that largely duplicates existing FERC authority under

Section 215 of the Federal Power Act and could substantially undermine the existing reliability standards regime. We question whether FERC has the technical or intelligence-handling expertise to exercise such a broad new authority. Operationally, this new authority could result in the establishment of potentially conflicting or different cybersecurity standards in the U.S. and Canada. We urge the Subcommittee to focus its attention on the immediate, narrow issues at hand: 1) the need for the federal government to issue emergency orders very quickly if the bulk power system is under an imminent threat of cyber attack; and 2) the need for the electric power industry to receive timely, actionable information to facilitate responses to such threats.

GRID Act Section 2(b): Emergency Response Measures

The draft gives FERC new authorities to issue emergency orders if the President notifies the Commission that an "imminent grid security threat" exists. When the federal government has actionable intelligence about an imminent cyber threat to the electric grid, there won't always be time for classified industry briefings or thorough development of mitigation measures. In these limited circumstances, the federal government should have the authority to direct the electric power industry on the needed emergency actions until the threat ends, is mitigated or a one-year period has elapsed.

GRID Act Section 2(c): Measures to Address Grid Security Vulnerabilities

The draft gives FERC the authority, if it determines there is a grid security vulnerability that existing NERC reliability standards do not address, to issue a rule or order requiring any owner, operator or user of the U.S. bulk-power system to implement measures to protect against the vulnerability. The draft encourages FERC to consider recommendations from NERC. The draft also lists three specific vulnerabilities FERC

must address with this new authority[1]. This section and the new authority it seeks to provide to FERC are very concerning to our industry. This subsection represents a fundamental alteration of the Section 215 reliability regime that could result in duplicative, conflicting, or unworkable reliability standards across the diverse North American grid.

Furthermore, FERC already has the authority to instruct NERC to develop or modify a standard on any topic, including but not limited to, the three vulnerabilities listed in the draft GRID Act. Section 215(d)(5) reads:

> "The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."

Vulnerabilities are potential events with longer lead times and without the accompanying intelligence that the vulnerability will be exploited with impact. Vulnerabilities present a lower urgency and risk level than threats and the debate over how to address them should recognize that vulnerabilities alone do not adversely impact the reliability of the electric grid. Infrastructure users, owners and operators take vulnerabilities very seriously and should act appropriately to address vulnerabilities before any are potentially exploited. Electric infrastructure owners and operators have

[1] At subsection 2(c)(2), the draft instructs FERC to issue a rule or order to any user, owner or operator of the U.S. bulk power system requiring the implementation of measures to protect the bulk-power system against a vulnerability known as "Aurora." Subsection 2(c)(4) instructs the Commission to issue an order to NERC to produce a standard on geomagnetic storms. Subsection 2(c)(5) instructs the Commission to issue an order directing NERC to produce a standard on the availability of large transformers.

every incentive - ranging from financial considerations to the fundamental obligation to serve our customers with reliable, safe and affordable power - to take the necessary steps to protect the grid from threats and vulnerabilities.

If intelligence agencies or FERC have identified grid vulnerabilities or threats, industry needs to be made aware of them immediately so necessary actions can be taken. The electric industry wants a safe, secure and reliable grid and we need access to timely and actionable federal government intelligence to help us to do that job to the best of our abilities.

GRID Act Section 2(g)(3): Security Clearances and Communication

Our sector can be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats and vulnerabilities because of limitations on its access to classified information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. The government is able to detect threats, evaluate the likelihood or risk of a malicious attack, and utilize its expertise in law enforcement. Industry participants accountable for protecting critical infrastructure can respond to threats and address vulnerabilities even more effectively with timely, clear and actionable information from government partners.

On the other hand, the electric industry is experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operated. The electric industry is uniquely positioned to understand the consequences of a potential malicious act and the proposed mitigating actions needed to prevent such exploitation, including ensuring

against unintended consequences of remedial actions. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more reliable and secure electric grid for the benefit of our customers.

In order for the electric power sector to partner effectively with government to protect the grid when vulnerabilities or threats arise, we need timely, actionable information and intelligence from government. Additional selected experts in the electric industry need to have higher levels of security clearances so that trusted people within our sector with industry knowledge can assist the federal government in fashioning a response to threats and vulnerabilities and help direct needed industry actions.

The draft legislation seeks to improve information sharing between the federal government and the electric power industry, with provisions aimed at expediting the acquisition of crucial security clearances to key personnel and requiring the distribution of timely and actionable information regarding threats and vulnerabilities. We appreciate the Subcommittee's support on this critical aspect of grid protection.

Conclusion

Thank you for the opportunity to testify at today's important hearing. The electric industry looks forward to working with the Subcommittee and full Committee to fashion legislation that will maintain the industry-government partnerships that are already making the grid more secure and supply the additional narrow authority that is needed if a severe and imminent cyber threat emerges.

Mr. WHITFIELD. Thanks, Mr. Lawson.

Mr. Kramer, you would agree then that in the interest of national defense that additional Federal authority is necessary?

Mr. KRAMER. Yes, sir, I think it is absolutely required.

Mr. WHITFIELD. OK. And Mr. Cauley, you mentioned in your testimony, I believe, that you didn't think it was necessary for NERC to develop standards to ensure the availability of large transformers, and I am certainly not an expert in that area but it is my understanding that the availability of large transformers is one of the key issues out there and I was just curious if you would elaborate on your position on that.

Mr. CAULEY. Thank you, Mr. Chairman. I do take the issue of spare equipment and transformers very seriously from physical attack, cyber or GMD, and it is a major issue. So I think we don't have enough information yet to know what the standards should be in terms of how much equipment and where it would be located and how we would transport it, so if I said something opposing future standards on spare equipment, I may have misspoke and I will have to go look in my written testimony. But it is a key issue, and we are dealing with it today with some industry experts on a task force that are looking at likely scenarios, what would the need be, how would we move the equipment, so we are trying to find a technical solution to the problem before we tackle the issue of whether there should be a standard or not.

Mr. WHITFIELD. So are these transformers manufactured in the United States today?

Mr. CAULEY. The vast majority of them have been manufactured overseas and continue to be. There is some recent activity to bring some onshore but the vast majority are manufactured overseas.

Mr. WHITFIELD. Now, Mr. Lawson, I am sure you heard the testimony today that in addition to the bulk electric system, that distribution should be included in this, and of course, rural electric coops are quite involved in distribution, so would you disagree with that, or what would be your position?

Mr. LAWSON. Well, we believe that the legislation before us should focus on the bulk power system. Distribution is handled at the local level, whether that be State or local municipality level or with the local board of a cooperative, and we don't think it needs to be extended to the Federal level.

Mr. WHITFIELD. But how do we address the potential problem in some of these large metropolitan areas that was mentioned?

Mr. LAWSON. With regard to the distribution facilities in the large metropolitan areas?

Mr. WHITFIELD. Yes.

Mr. LAWSON. I think there is one definition in the NERC glossary that is being worked on today, and that is the definition of bulk electric system. That definition is looking at how and what should be included under bulk electric system, and one of the issues that the commission has directed the industry through NERC to review is how those facilities in large metropolitan areas are covered, and I think the direction that that drafting team is going in that I am a member of is covering more facilities in those metropolitan areas than are currently covered under the existing NERC BES, bulk electric system, definition.

So I think things are changing and a draft of that definition was recently out for public comment, and it is now moving on to the second draft phase, so I think there will be changes in that area.

Mr. WHITFIELD. So Mr. Cauley, do you or Mr. Kramer have any comments on that particular issue?

Mr. CAULEY. Just a couple, Mr. Chairman. The industry has a very long history of the issue of local service and distribution being dealt with with the ratepayers in the local jurisdiction and obviously the States and other local jurisdictions, so I think any effort to encroach on that through Federal legislation I think should just be taken carefully in consultation with the States.

On the issue of the military bases, which was part of the earlier testimony, I think there is an opportunity to have enhanced discussions between the utility company and the military bases to say do they have what they need, do they need more backup generators, do they need more lines coming in to the base, so I think there is opportunity for those discussions to take place. I will end there. Thanks.

Mr. WHITFIELD. Mr. Kramer?

Mr. KRAMER. I would disagree with both of these gentlemen. First of all, I think we have the smart grid becoming ever increasingly a greater part of the electric power system, and the smart grid means that from the consumer side, from the distribution side, you are going to have increasing vectors that allows for cybersecurity attacks, and those could be national security attacks, so I think that we need to have an overall Federal standard that protects against that, and NIST is working on that. I don't actually think they have done enough but at least they have done something. But I think we need to put that into play, so I would very strongly encourage the committee to expand its jurisdiction.

With respect to the military bases and the like, I think Mr. Stockton was pretty clear, they don't have enough, and it is not just the bases themselves. If you think about the military, for example, the entire critical infrastructure, transportation infrastructure, the telecommunications infrastructure, all of these depend upon electricity. So even if the bases themselves had electricity, the DOD simply couldn't operate without transportation, without telecommunications and the like, and I think we really need to have something done about that.

Mr. WHITFIELD. Mr. Lawson?

Mr. LAWSON. Just to add to that, on the military bases, the best way to effect change and improvements is at the local level between the military installation, commander and the leadership of the utility supplying that military installation. Those relationships exist today. They are typically very good relationships, and if there are additional levels of reliability, security that are needed, it is very important for the military installation leadership to let the utility know and they can work jointly towards providing that.

With regard to the smart grid, the industry is not implementing smart grid facilities carelessly. They are doing it carefully and keeping security very much in mind in many different ways. We are also working very closely and as much as we can with the vendor community to try to explain to them what levels of security we need and what levels of security already exist in their equipment

today, so it is something that we are focused on and not doing carelessly.

Mr. WHITFIELD. Thank you all. My time is expired.

Mr. Rush, you are recognized for 5 minutes.

Mr. RUSH. Thank you, Mr. Chairman. This has been quite interesting.

Mr. Cauley, I would like to ask you about imminent threats to the grid and also long-term vulnerabilities as well. Let us say our intelligence agencies learn of an imminent threat to the grid from terrorists. How would you characterize NERC's authority to step in and address that threat on a real-time basis?

Mr. CAULEY. We have the ability to acquire that information through working with various intelligence agencies, which we do continuously to get the information digested into what it means in terms of impact on the industry and issue various levels of alerts, and we have done that. We issued one back just in April which we turned around within a day. So depending on the urgency, we can turn them out in hours or days. I think as I pointed out in my testimony, we have different levels. Some are just informational, some are recommendations, and there are essential actions which we have also been able to put out. The essential actions are mandatory under our rules but they are not enforceable from a legal sense in terms of any sort of penalties and sanctions, and that was why I was suggesting in my testimony that that would be one opportunity to improve the toolkit that we have to get timely, actionable information out to industry.

Mr. RUSH. And would this apply if there were imminent and severe threat also?

Mr. CAULEY. This would apply really to any known threat or vulnerability where there was a high degree of urgency like we needed to get information out either within hours or days or weeks, and I think that is a much preferred approach. Everyone keeps referring to our standards. Well, our standards were not meant to solve a problem in 3 days or 3 weeks. They are meant to be long-enduring, around for years and years. The alert system is meant to solve these urgent actions that you are describing here.

Mr. RUSH. Does FERC have sufficient authority at this point?

Mr. CAULEY. I believe in the area of vulnerabilities in terms of, for example, whether it is Aurora or spare transformers, I believe under section 215 that Congress intentionally provided FERC authority to direct the ERO to produce a standard that would solve a problem. So under my reading of the plain language of section 215, the FERC has the ability to direct us to——

Mr. RUSH. Mr. Kramer, do you agree with that?

Mr. KRAMER. I totally disagree, and I will give you an example. This committee has heard about Stuxnet, obviously, and Stuxnet is not a classified problem. Semantic organizations among many others has issued a very detailed set of reports on this. It is a threat. It is a very, very, very severe threat that we have to think about, and the vulnerability exists throughout the electric grid system because it is the same kind of control mechanisms that Stuxnet attacked that are the type that are involved in the electric grid, and it is sitting out there, so to speak, as a blueprint for anyone to use—now, I couldn't use it, but any capable cyber adversary. So I

think that that would be an example of what I would call a severe threat. It is not imminent but I think that something needs to be done about that right now, and I think it needs to be done promptly, and from my perspective, and I said, as we do in other kinds of legislation, I would rather have the opportunity for the industry to comment but for the Federal Government, be it the FERC or the DHS, but some Federal agency to determine what standards are necessary, what actions need to be taken promptly and to cause those to be taken under a mandatory system.

Mr. RUSH. Mr. Lawson, would you give us your opinion on this?

Mr. LAWSON. First of all, as I said in my statement, the industry strongly supports the alert process. I am not aware of another tool out there today that can get information out to approximately 2,000 utilities within hours or a day or two with specific information about how a threat or a vulnerability or anything that specifically relates to the electric utility industry. So I think the alert process is a very critical one and one that we need to keep utilizing.

Also, under the alert process, there are three levels. The base level is advisory, the middle level is recommended action, and the most serious level is essential action. And I can tell you that the industry reacts very strongly to these alerts because we know that they are communicating very important information to the industry and that under the top two levels of alerts, you will be required to provide NERC with an update on what you have done with regard to that alert, and those reporting requirements are mandatory, and then they are summarized and provided to FERC. So the industry takes these very seriously and the top-level alert, essential action, has not yet been utilized. So only the advisory and the recommended action have been utilized, and both of those levels have been taken very seriously by the industry, and I am sure essential action would be taken exactly the same.

Mr. RUSH. Mr. Chairman, I just want to ask one other question.

So let me just ask you this. All three of you can respond or anyone can respond. What I am hearing here is that in the event of an imminent, severe, catastrophic cyber attack on the electrical grid system here in this country where there could be vast harm done to the American people, are you saying, am I correct in understanding that you are saying that the Federal Government—or let me ask the question this way: Who are the American people going to hold responsible for their protection to solve the problem and to protect them? Are they going to hold the Federal agencies or the industry responsible, in your opinion?

Mr. CAULEY. Congressman Rush, I mean, first of all, to distinguish some time horizons, first of all, if there is an imminent emergency like planes flying on 9/11 that are going to cause disaster, NERC and I think the industry supports some government agency having strong, immediate authority under those kind of circumstances—the Nation is in trouble, somebody has to be in charge—I think we support that. And I think the other issues I think where we get a little bit of difference of opinion but it is not as bad as it sounds, actually, is on dealing with the things we have a longer time to think about and respond to, and all we are saying is that we think that the FERC has for longer-term issues like

spare equipment—we are not going to solve spare transformers tomorrow, it is going to take probably years to resolve that—is that we have the authorities we have now, and I think we could strengthen the gap in the middle between dire emergency right now and things that might take months to solve. In the interim, we have our alert system and all we need is a little more authority to make those mandatory in some cases. When I testify here today, I am not here testifying against authority for FERC. We work with FERC today as a partner in developing our standards. They review them and approve them, and I view going forward that we would continue to work with FERC, that anything that we can do to help the industry know what they have to do and whether it is mandatory or not, that we would do that in partnership with FERC.

Mr. WHITFIELD. Mr. Terry, you are recognized.

Mr. TERRY. Thank you.

To follow up on that, have you, Mr. Cauley, read the GRID Act or the proposal, the draft? So as it is written now, my assumption is, you don't support it? Is that accurate, you wouldn't support it as written?

Mr. CAULEY. I applaud the committee for taking initiative——

Mr. TERRY. I have short time. Yes or no?

Mr. CAULEY. I support parts of it, not the entire——

Mr. TERRY. The jurisdictional part, you have a problem with?

Mr. CAULEY. With the vulnerabilities being unnecessary, that is correct.

Mr. TERRY. Mr. Lawson, same question.

Mr. LAWSON. We support narrow authority for the Federal Government with regard to imminent cyber threats.

Mr. TERRY. So that is a no? OK. I appreciate that. I think we have more work to do than I anticipated before this hearing.

Mr. Kramer, I want to spend the rest of the time with you. Do you keep track or is there reporting of hacking attempts to your office or any office that you know of?

Mr. KRAMER. Just so we are clear, I am a former Assistant Secretary so I am testifying in my individual capacity here.

Mr. TERRY. All right.

Mr. KRAMER. So I read the—there are plenty of reports on hacking that are in the open press and there are plenty of reports on hacking that are maintained by a lot of entities, and I think——

Mr. TERRY. Electrical generation?

Mr. KRAMER. Including electrical, and the Night Dragon point was made to this committee as an example.

Mr. TERRY. I participated in a demonstration at our local generator that was able to track hacking attempts within the last 24 hours, and I think there was six or seven. Most they have been able to track back to a certain university in China, but we won't go into that for this hearing. Now, they were mostly—how do I say this—for fun. It was their practice of seeing how they can enter into the system, and not for nefarious purpose, although we don't know that when they are trying to do it, when they are trying to hack the system, and that is what concerns me and this committee is what we can do to strengthen our system against those hacks.

And by the way, just two questions to you, Mr. Kramer, in my 2 minutes left. Generally, what should electrical generation compa-

nies be doing to best ensure that their systems can't be hacked into? And then on the electrical generation itself, there have been some side discussions on electrical generation, whether the more critical defense bases or buildings should go off grid, totally reliant and with the small module nuclear reactors may allow them to do that. You have a minute and a half to comment on both those questions.

Mr. KRAMER. I will make three points, sir. First of all, with respect to the issue of serious attack, one of the things that a serious attack would have to do would be reconnaissance. You won't just attack without substantial reconnaissance, so the reconnaissance or the activities that you are talking about are quite consequential and would be part of any serious attack and so dealing with those early on is just as important as dealing with the set of issues, you know, so to speak, when the attack occurs.

Second, with respect to what the industry ought to do, there are a number of standards set forth, both the NERC itself, FERC, DOE and others have written out which I think one is called, well, 20 critical activities that were put out by one of the cybersecurity groups. Those are what you might call very good hygiene, and one of the critical things that I think needs to be done is that there has to be a greater amount of protection provided to the control system portion of the grid than to what is called the corporate portion of the grid, and I also think that there need to be what I would call advanced capabilities developed so that you can isolate the control portion of the grid from the corporate capabilities and from vendors and others who have to send things in. I think there will need to be, as I mentioned, integrity capabilities that do exist now at the bench level, so to speak, at the demonstration level but are not out there throughout the grid, and I think that the critical parts of the industry, Mr. Markey mentioned that—I don't have his exact figures but roughly 29 percent, if I remember right, of the grid was considered critical by the industry. I think it is a much larger amount than that, so I think you have to have more significant.

With respect to the bases again, I want to make the point that even if the bases themselves have electricity and there are actions going on, I can't tell you what the acronym stands for anymore but it is called SPIDERS. It is a demonstration program, and this is non-classified—you can look it up on Google—to make the bases more self-sufficient, and the DOE has a so-called SPIDERS program at three or four different bases. But even if the bases themselves have electricity, the DOE relies on telecommunications capabilities of the country, it relies on the transportation capabilities of the country, it relies on water, it relies on gas pumps and the like, and all those rely on electricity. So there is no possibility whatsoever that you could have an effective defense unless you have electricity available beyond the bases. In addition, that happens to also be true overseas, which is a different topic that the chairman raised, but it goes beyond the question.

Mr. WHITFIELD. Mr. Rush, do you have anything else you want to touch on?

Well, that concludes today's hearing. We appreciate your being here, and I am sure we are going to continue to be in touch with you as we move forward on this legislation, and we will keep the

record open for 10 days for additional materials, and thank you all very much, and that concludes today's hearing.

[Whereupon, at 4:25 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Opening Statement of Chairman Fred Upton
"Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act"
Subcommittee on Energy and Power
May 31, 2011

The subject of this hearing – protecting the electric grid – is an issue of critical importance to our national security. And it is of special importance to me, having worked last year with Mr. Markey on the "Grid Reliability and Infrastructure Defense Act," or the "GRID Act." We proposed that legislation in response to growing concerns regarding the security of the nation's bulk power system. Building on last year's progress, I am eager to hear from today's witnesses about any changes that are needed to strengthen the proposal. We will continue working in a bipartisan manner to produce the best legislation we can to bolster the security of the grid.

The discussion draft released for today's hearing is identical to last year's GRID Act, making it an excellent starting point for this Committee's efforts to address grid security.

The GRID Act gives the Federal Energy Regulatory Commission (FERC) the authority to respond to an imminent attack. The risk of such an attack is real, and the implications for our national security and our economy will be far-reaching if we do not act now to adequately protect the grid.

The grid's reliability and security requirements currently are formed by the North American Electric Reliability Corporation (NERC). While NERC and industry have together made significant strides to address reliability and

cybersecurity concerns, NERC's deliberative process is not set up to quickly respond to imminent threats identified by federal authorities.

NERC's open stakeholder process can take months or years to develop and implement a mandatory standard. Moreover, confidential national security information could be compromised through some of the NERC transparency requirements. And NERC-issued standards and alert advisories are generally applicable to the entire electric industry, which makes it nearly impossible to address specific threats and vulnerabilities.

In contrast, the GRID Act would grant FERC the authority to address narrow grid threats and vulnerabilities tailored to specific entities and assets, thus assuring quick notice to – and prompt action from – owners and operators of the bulk power system.

Members of this Committee would not grant additional authority to a federal agency without careful consideration. However, where our national security and national economic interests are at stake, it is a step we are willing to consider to ensure the safety of all Americans and the reliability and affordability of our electricity supply to drive America's economy.

Accordingly, there is strong justification in this limited circumstance to arm FERC with tailored new authority to act in the face of imminent threats to the grid and to identify and mitigate vulnerabilities to the bulk power system.

I look forward to today's discussion and thank the witnesses for their participation on this critical national security issue.

○