

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: 10 CFR 2.206 Petition Review Board
RE Thomas Saporito

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Monday, September 10, 2012

Work Order No.: NRC-1834

Pages 1-73

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

10 CFR 2.206 PETITION REVIEW BOARD (PRB)

PUBLIC MEETING

+ + + + +

MONDAY

SEPTEMBER 10, 2012

+ + + + +

The public meeting was held at 11555 Rockville Pike, One White Flint North, Rockville, Maryland, at 12:00 p.m., Ho Nieh, Chairperson of the Petition Review Board, presiding.

PETITIONER: THOMAS SAPORITO

PETITION REVIEW BOARD MEMBERS

HO NIEH, PRB Chair, NRR/DIRS

TANYA M. MENSAH, Petition Manager for 2.206

petition, NRR/DPR/PGCB

JOSEPH DeCICCO, FSME 2.206 Coordinator*

MARIO R. FERNANDEZ, NSIR/DSO/RSOB

NORMA GARCIA-SANTOS, NMSS 2.206 Coordinator*

LINDA HOWELL, RIV/ORR

TIM MOSSMAN, NRR/DE/EICB

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 PERRY PEDERSON, NSIR/DSP/ISCPB

2 NICOLE COLEMAN, OE (Advisor)

3 CARRIE SAFFORD, OGC (Advisor)

4

5 NRC HEADQUARTERS STAFF PRESENT:

6 RONALD ALBERT, NSIR/DSO/RSDB

7 JOE DEUCHER, NSIR/DSP/CSIRB

8 MARK LOMBARD, NMSS/SFST

9 DAVID PELTON, NRR/DPR/PGCB

10 BLAKE PURNELL, NRR/DPR

11 ANDREA RUSSELL, NRR/DPR/PGCB

12 ALEX SAPOUNTZIS, NSIR/DSP/FCTSB

13

14 ALSO PRESENT:

15 MATT DELLON, Pacific Gas & Electric*

16 STEVEN HAMRICK, FPL*

17 JEFF LeCLAIR, Xcel Energy*

18 DAVID REPKA, Winston & Strawn/Pacific Gas &

19 Electric

20 CRAIG ROSEN, Pacific Gas & Electric*

21 JAMES ROSS, GE Hitachi

22

23 *Participating via teleconference

24

25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

T A B L E O F C O N T E N T S

| | |
|--------------------------------------|----|
| Welcome and Instructions - T. Mensah | 4 |
| Introductions - Participants | 6 |
| Background from Chairman | 10 |
| Presentation from Petitioner | 17 |
| Question & Answer Period | 64 |
| Adjourn | 73 |

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

P R O C E E D I N G S

1
2
3 MS. MENSAH: This is Tanya Mensah with the
4 NRC. We are proceeding with this meeting. I would like
5 to thank everyone for attending this meeting.

6 You're here today to allow the Petitioner,
7 Mr. Thomas Saporito, Senior Consultant for SaproDani
8 Associates to address the NRC Petition Review Board,
9 also referred to the PRB, regarding the 2.206 Petition
10 dates July 30, 2012. The Petitioner requests that the
11 NRC take enforcement-related action against all NRC
12 licensees as a result of information provided on a
13 Bloomberg News Agency broadcast which described a cyber
14 security incident at Diablo Canyon.

15 I am the petition manager for the Petition
16 and Mr. Ho Nieh is the Petition Review Board Chairman.

17 As part of the PRB's review of the Petition,
18 the Petitioner was offered an initial opportunity to
19 address the PRB to provide any relevant additional
20 explanation and support for the Petition. At the
21 request of Mr. Thomas Saporito, he requested this
22 opportunity to provide supplemental information in
23 support for the Petition before the PRB meets internally
24 to make the initial recommendation to accept or reject
25 the Petition for review.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 This meeting is scheduled for two hours,
2 from 12:00 noon until 2:00 p.m. The meeting is being
3 recorded by the NRC Operations Center and will be
4 transcribed by a court reporter. The transcript will
5 become a supplement to the Petition. Prior to placing
6 the transcript in ADAMS, the PRB will review the
7 transcript that it does not contain any allegations or
8 sensitive information.

9 For those at the NRC Headquarters, we have
10 public meeting feedback forms that you are welcome to
11 fill out. You may either leave them here following the
12 meeting or mail them back. They are already post-paid.

13 If you are participating by phone and would
14 like to leave email feedback on this public meeting,
15 please forward your comments to me by email at
16 tanya.mensah@nrc.gov. My email address is also on the
17 meeting notice.

18 I would like to open this meeting with
19 introductions of the NRC meeting participants. I ask
20 that all of the participants clearly state for the record
21 your name, your position and your organization.

22 For those here in the room, please speak
23 up so that those on the phone can hear clearly and so
24 that the court reporter can accurately record your name.

25 I will start with myself and the other NRC participants

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 here in the room.

2 I'm Tanya Mensah. I work in the Office of
3 Nuclear Reactor Regulation, Division of Policy and
4 Rulemaking. I am the 2.206 Coordinator and the Petition
5 Manager for this Petition.

6 CHAIRMAN NIEH: I am Ho Nieh. I'm the
7 Director of the Division of Inspection and Regional
8 Support in the Office of Nuclear Reactor Regulation.
9 And I'll be serving as the Petition Review Board Chair.

10 MS. HOWELL: And I'm Linda Howell. I'm the
11 Chief of the Response and Coordination Branch in the
12 Region IV Office in Texas.

13 MR. FERNANDEZ: Mario Fernandez. I'm a
14 cyber security specialist at the Nuclear Security and
15 Incident Response Office, Division of Security
16 Operations.

17 MR. PEDERSON: Perry Pederson. I'm a cyber
18 security specialist with the same office as Mario,
19 Nuclear Security and Incident Response, Division of
20 Security Policy.

21 MS. COLEMAN: I'm Nicole Coleman,
22 Enforcement Specialist in the Office of Enforcement.

23 MS. SAFFORD: I'm Carrie Safford. I'm in
24 the Office of General Counsel in Materials, Litigation
25 and Enforcement Division.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. MOSSMAN: Tim Mossman. I'm an engineer
2 in the Instrumentation and Control Branch of the Office
3 of Nuclear Reactor Regulation.

4 MR. PELTON: David Pelton, Branch Chief in
5 the Division of Policy and Rulemaking, Office of Nuclear
6 Reactor Regulation, responsible for the 2.206 process.

7 MR. PURNELL: Blake Purnell, also with the
8 Division of Policy and Rulemaking in the Office of
9 Nuclear Reactor Regulation.

10 MR. SAPOUNTZIS: I'm Alex Sapountzis,
11 Senior Project Manager in the Office of Nuclear Security
12 Incident Response. I work in the Fuel Cycle
13 Transportation Security Branch.

14 MR. RUSSELL: Andrea Russell, Project
15 Manager, Division of Policy and Rulemaking, Nuclear
16 Reactor Regulation Office.

17 MR. DEUCHER: I'm Joe Deucher, Nuclear
18 Security Incident Response, Division of Security Policy,
19 Cyber Security Incident Response branch.

20 MR. REPKA: David Repka with the law firm
21 of Winston and Strawn in Washington, D.C. and I'm outside
22 counsel to Pacific Gas & Electric Company.

23 MR. ROSS: James Ross, GE Hitachi.

24 MR. LOMBARD: Mark Lombard. I'm the
25 Director of Spent Fuel Storage and Transportation in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the Office of Nuclear Material Safety and Safeguards
2 in the NRC.

3 MS. MENSAH: That completes the
4 introductions of the NRC staff and also members of the
5 public in the room. Do we have any NRC staff from
6 Headquarters on the phone?

7 MR. DeCICCO: Yes. This is Joseph DeCicco.
8 I'm the 2.206 Petition Coordinator for the Federal and
9 State Materials and Environmental Management Program
10 Office at the NRC.

11 MS. GARCIA: And I'm Norma Garcia. I'm the
12 2.206 Petition for the Office of Nuclear Material Safety
13 and Safeguards.

14 MS. MENSAH: Thank you. At this time, we
15 have a number of licensees dialing in to listen to the
16 public meeting. We'll have a roster playback of the
17 NRC Operations Center so that we can hear all the names
18 and organizations of those joining us by phone.

19 (Roster playback.)

20 Is the NRC Operations Center on the line?

21 MR. LeCLAIR: Jeff LeClair with Xcel
22 Energy.

23 MR. HAMRICK: Steve Hamrick, NextEra
24 Energy.

25 MR. ROSEN: Craig Rosen and Matt Dellon,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Pacific Gas & Electric.

2 (Roster playback complete.)

3 MS. MENSAH: Mr. Saporito, at this time,
4 would you please introduce yourself for the record?

5 MR. SAPORITO: My name is Thomas Saporito.
6 I'm Senior Consultant with Saprodani Associates based
7 out of Jupiter, Florida.

8 MS. MENSAH: Thank you.

9 Again, I would like to emphasize that we
10 each need to speak clearly and loudly to make sure that
11 the court reporter can accurately transcribe this
12 meeting. If you have something that you would like to
13 say, please first state your name for the record.

14 For those dialing in, please remember to
15 mute your phones to minimize any background noise or
16 distractions. If you do not have a mute button, this
17 can be done by pressing the keys *6. To unmute, press
18 the *6 keys again. Please note that the Operations
19 Center has already muted the phones for people who are
20 not addressing the PRB. Those lines will be unmuted
21 during the public comment portion of this meeting.

22 Thank you. At this time, I'll turn it over
23 to our PRB Chairman, Mr. Ho Nieh.

24 CHAIRMAN NIEH: Okay. Thank you, Tanya.
25 And good afternoon everybody. Thanks for being here

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 today to discuss this 2.206 Petition submitted by Mr.
2 Thomas Saporito, Senior Consultant for SaproDani
3 Associates out of Florida.

4 To give a little bit of background about
5 the process we're in, Section 2.206 of Title 10 of the
6 --

7 OPERATOR: This is the Headquarters'
8 Operations Officer. We're not picking up the recording
9 very well. Can you speak closer to the phone please?

10 CHAIRMAN NIEH: I sure can. Okay.

11 We'll start with some background about the
12 process we're in. Section 2.206, Title 10 of the Code
13 of Federal Regulations enables any person to file a
14 petition to the NRC for an enforcement-related action
15 to either modify, suspend or revoke an NRC license or
16 take any other appropriate enforcement action to resolve
17 an issue. The NRC staff's guidance is contained in
18 Management Directive 8.11 which is publicly available.

19 The purpose of today's meeting is to give
20 the Petitioner an opportunity to provide additional
21 support and information on the Petition before the
22 Petition Review Board's initial consideration and
23 recommendation. The purpose of this meeting is it is
24 not a hearing nor is it an opportunity for the Petitioner
25 to question or examine the Petition Review Board on its

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 views or the merits of the Petition and the Petition
2 Review Board will not be making any decisions regarding
3 the merits of the Petition at this meeting.

4 However, following the meeting, the
5 Petition Review Board will conduct its internal
6 deliberations. And the outcome of that internal meeting
7 will be discussed with the Petitioner.

8 The Petition Review Board typically
9 consists of a chairman, usually a manager at the Senior
10 Executive Service level at the NRC. It has a petition
11 manager and other members of the Board are determined
12 by the NRC staff based on the content of the information
13 and the support that the Board would need.

14 At this time, I'd take a moment to introduce
15 the Board. As I said, I'm Ho Nieh, the Petition Review
16 Board Chair. Tanya Mensah whom you already met is the
17 Petition Manager. And the technical staff supporting
18 the Petition Review Board or PRB includes the following:
19 Mr. Perry Pederson of the Office of Nuclear Security
20 and Incident Response; Mr. Mario Fernandez from the
21 Office of Nuclear Security and Incident Response; Mr.
22 Tim Mossman from the Office of Nuclear Reactor
23 Regulation; Ms. Linda Howell from NRC's Region IV Office
24 in Texas; and we also obtain advice from the Office of
25 the General Counsel who is represented by Ms. Carrie

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Safford today as well as the Office of Enforcement being
2 represented by Ms. Nicole Coleman.

3 In addition, we are also coordinating with
4 several other NRC offices with representatives from the
5 Office of Federal and State Materials and Environmental
6 Management Programs, the Office of Nuclear Material
7 Safety and Safeguards and the Office of New Reactors.

8 And we have these offices involved to take a look at
9 whether your petition affects or relates to any other
10 NRC licensed facilities outside of power reactors.

11 As described in our process in Management
12 Directive 8.11, the NRC may ask clarifying questions
13 to the Petitioner in order to better understand your
14 presentation and to reach a decision on whether to accept
15 or reject the Petitioner's request for review under the
16 2.206 process.

17 Also described in our process, licensees
18 have been invited to participate in today's meeting.
19 There are several licensees on the bridge. This is to
20 ensure that they understand any concerns about their
21 facilities or activities.

22 While licensees may also ask questions to
23 clarify the issues raised by the Petitioner, I want to
24 stress that the licensees are not a part of the Petition
25 Review Board decision-making process.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I'll briefly summarize the Petition Review
2 Board's understanding of the scope of the Petition that's
3 under consideration today. Tanya gave some background,
4 but I'll just cover it again for completeness.

5 On July 30, 2012, Mr. Thomas Saporito of
6 SaproDani Associates who we will refer to as the
7 Petitioner submitted a petition under Title 10 of the
8 Code of Federal Regulations, Part 2.206. The Petitioner
9 requests that the NRC

10 (1) seek escalated enforcement action
11 against all NRC licensees and suspend or revoke the NRC
12 licenses granted to the licensees for operation of any
13 nuclear reactor or facility;

14 (2) issue a notice of violation with a
15 proposed civil penalty against the licensees in the total
16 amount of \$100,000; and

17 (3) issue a confirmatory order to the
18 licensees requiring the licensees to take their nuclear
19 reactors and/or facilities to a cold shutdown mode of
20 operation until specific actions described in the
21 Petition have been completed.

22 I'll take a moment to also discuss some of
23 the NRC activities related to this Petition that have
24 occurred to date.

25 As I mentioned, on July 30th, the Petition

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 was submitted.

2 On July 31st, Ms. Tanya Mensah, the Petition
3 Manager, contacted Mr. Saporito to inform him of the
4 NRC's receipt of the Petition. Mr. Saporito requested
5 an opportunity to address the Petition Review Board in
6 a public meeting which is the purpose of today's meeting.

7 On August 27th, the Petition Review Board
8 members and advisors met to discuss the Petitioner's
9 request for immediate action. And though an immediate
10 action wasn't explicitly called out for in the Petition,
11 we treated your request as if it were in immediate action.

12 And we looked as far as an immediate action goes whether
13 it should be required that all NRC licensees take their
14 nuclear reactors and/or facilities to a cold shutdown
15 mode of operation as described in the Petition.

16 In an email dated September 5, 2012, the
17 Petition Manager informed the Petitioner of the Petition
18 Review Board's decision to deny the request for immediate
19 action. Specifically, in accordance with 10 CFR 73.54,
20 Protection of Digital Computer and Communication Systems
21 and Networks, each licensee shall protect digital
22 computer and communication systems and networks
23 associated with:

24 (1) safety related and important to safety
25 functions;

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 (2) security functions;

2 (3) emergency preparedness; and

3 (4) support systems and equipment which are
4 compromised with adversely impact safety or security.

5 That particular regulation is known as the
6 NRC Cyber Security Regulation. And when we considered
7 your request for immediate action we looked at what those
8 specific requirements required of the NRC licensees with
9 respect to submitting a cyber security plan. The NRC
10 Petition Review Board and its advisors were made aware
11 that licensees had submitted their cyber security plans
12 for NRC review. And those reviews are in progress and
13 inspections would be underway to assess those plans.
14 The Petition Review Board determined that there was
15 insufficient information at this time to grant any
16 immediate actions to place the power reactor facilities
17 in a cold shutdown condition.

18 As a reminder for the meeting,
19 Participants, we want to make sure that you all identify
20 yourself before you speak as again this meeting is going
21 to be transcribed. And that transcription of the
22 meeting will be made publicly available. It will help
23 the Petition Review Board go back over the discussion
24 at the meeting while it makes its decision.

25 I also want to mention that the NRC staff

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 had verified that there was no security-related
2 information contained within the Petition. And since
3 this is a public meeting I'd like to remind the PRB
4 members, the NRC licensees that are on the phone, the
5 Petitioner and other meeting participants of the
6 importance to refrain from discussing any NRC
7 security-related information during the meeting.

8 With that, Mr. Saporito, I'd like to turn
9 it over to you to have you provide any additional
10 information you believe the PRB should consider as part
11 of this petition. Starting now, you'll have roughly
12 one and a half hours as you requested to make your
13 presentation.

14 MR. SAPORITO: Thank you, Mr. Chairman.
15 Again, my name is Thomas Saporito. I'm a Senior
16 Consultant with Saprodani Associates in Jupiter,
17 Florida. I am the one who authored the July 30, 2012
18 petition seeking enforcement action under NRC
19 Regulations 10 CFR, Part 2.206. And I'm aware that under
20 10 CFR 73.54 as you stated earlier there are in place
21 certain requirements and expectations from the NRC with
22 respect to its licensees for a nuclear power plant or
23 otherwise nuclear processing plant.

24 I'm going to show three or four short videos
25 in this presentation, explain the reliance of those and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 then I'm going to provide the PRB a brief chronology
2 of some issues/incidents related to cyber attacks. Then
3 I'm going to speak about the cyber threat with respect
4 to nuclear power plants. But to put all that into
5 perspective, I'm sure everybody has a key reflection
6 of what happened on 9/11 when the United States got
7 attacked by terrorists where the Trade Center buildings
8 were demolished with impact of some aircraft. That
9 incident brought to light the government's impotence
10 with respect to one agency collaborating with another
11 agency to protect the United States from such an attack.

12 Since that time, of course, we have born
13 the Homeland Security Department which is supposed to
14 coordinate with the FBI and CIA and various other law
15 enforcement agencies, many of which I'm not even aware
16 of. And since that incident happened, of course, we
17 haven't had another significant incident on our
18 homeland.

19 Nonetheless, the important lesson to be
20 gained from that in my view anyway is that the NRC needs
21 to start thinking outside the box. And the NRC needs
22 to do that in my view by collaborating with other federal
23 agencies such as the Federal Energy Regulatory
24 Commission and its licensees and licensee contractors
25 that have work in the transmission of nuclear power

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 across the United States.

2 The situation in this country is very grave
3 right now because in my view as a citizen in this country
4 and I'm sure my view is shared by many other Americans,
5 millions of our Americans, that the Congress is
6 dysfunctional at this time. If you have a Republican
7 look out the window of one of the Federal buildings and
8 say, "What a nice day it is," you've got a Democrat right
9 behind him saying "It's raining and it's stormy." It's
10 just become intolerant from a citizen's point of view.

11 The reason I bring that point up is because
12 they're a cyber terrorist law that's been kicking around
13 from one corner of Congress to the other and no one wants
14 to act on it. You have two Presidential candidates out
15 there taking personal attacks at each other rather than
16 resolving the serious issues facing this country at this
17 time.

18 It's part of politics I presume. But it's
19 very disturbing in my point of view.

20 And there are other issues such as the
21 fiscal financial cliff we're about to embark on and I'm
22 not going to go down that path. But the fact that the
23 Congress is dysfunctional is very serious because you
24 have this cyber terrorist law pending and you have other
25 legislation pending. And there's nobody up there that's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 going to make any decisions until after they find out
2 who is going to be the next president. And even then
3 they may not -- I mean, in my view, it doesn't really
4 matter who you put in that White House if the Congress
5 can't communicate and collaborate. Nothing meaningful
6 is going to change. I needed to put that background
7 into perspective to show you how serious this issue is.

8 When I grew up in Pittsburgh many years ago,
9 my dad sent me to the gas station to get some gas. He
10 wanted to cut the grass. He gave me this one gallon
11 container and a quarter. I went down there and filled
12 it up and brought him back ten cents change.

13 Well, things have changed since that time.

14 We used to leave our -- You know, people left their
15 doors open in their homes. They felt safe and secure.
16 And now you don't do that anymore.

17 And then you invented this thing called the
18 cell phone. People don't use it to talk to each other.

19 They would rather text and send emails and get on the
20 internet and all that kind of good stuff I guess that
21 is.

22 But this has now become a weapon for
23 terrorists to infiltrate nuclear power plants in our
24 country. I'll show you how that's going to be done.

25 And this is one of the reasons again that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it falls back on the Congress to start collaborating
2 and start passing some of these cyber terrorists law
3 so that the agencies like Homeland Security and the
4 Nuclear Regulatory Commission and the FBI and FEC. can
5 all start collaborating on how they're going to resolve
6 some of these issues so that this country can be
7 protected.

8 All right. This first video I'm going to
9 show -- Well, before I even get into that, let me just
10 briefly explain some of the enforcement actions I'm
11 requesting. I'm requesting that (1) the licensee
12 completes an independent assessment to fully understand
13 and correct the potential and/or real-life cyber
14 security threat posed by outside organizations. For
15 an example, the Comment group which is -- To my
16 understanding, it's a Chinese nation-based group.

17 (2) The licensee completes a comprehensive
18 evaluation of all nuclear safety-related plant equipment
19 and components which may be otherwise modified and/or
20 operated by remote means via internet access.

21 (3) The licensee completes, identifies and
22 removes any and all internet access points to all nuclear
23 safety-related plant equipment and/or components.

24 And (4) the licensee completes an
25 independent safety assessment to a third party

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 contractor to review all plant nuclear safety-related
2 equipment and/or components to ensure that such nuclear
3 safety-related systems and/or components are not
4 acceptable by an unauthorized entity via the internet.

5 Before I put this first video on, I'm not
6 placing myself here before as an expert in any stretch
7 of the imagination, but I can tell you from my experience
8 in dealing with the NRC and the regulations 10 CFR 73.54
9 does not go far enough to protect the licensees within
10 the NRC's jurisdiction. And I think that's going to
11 become very clear here very shortly.

12 This first video is a video produced by the
13 United States Government to the Bipartisan Policy Center
14 created for a cyber shockwave. It's a simulated cyber
15 attack on our nation. To defend against this attack,
16 a working group of high ranking former White House
17 Cabinet and National Security officials came together
18 with a mission to advise the President of the United
19 States.

20 (Cyber Shockwave video played.)

21 MR. SAPORITO: Okay. Some of the main
22 points that I take from this is that a cell phone could
23 be used as a weapon against the United States by a single
24 terrorist, a terrorist group or a state such as China,
25 Russia, Iran, whoever. But the fact of the matter is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the terrorists could be based out of China, linked into
2 a server out of Iran, launch a cyber attack on the United
3 States from Iran and the United States would want to
4 attack Iran believing that they were the host of the
5 attack which was not true in that particular hypothetical
6 scenario.

7 You can appreciate the difficulty in
8 responding to something like that. And, again, Congress
9 needs to put together a comprehensive cyber terrorist
10 bill and act and pass it quickly to address this issue.

11 But also related back to the Petition these
12 cell phones can be used, and we're going to get into
13 how, to access the grid, the National Grid, to access
14 nuclear power plants. You can put code in there to have
15 equipment self-destruct. I will show how that's done
16 here in these videos and in some of the text I'm going
17 to be talking about.

18 So although this presentation deals with
19 a scenario where they're advising the President on an
20 attack from another nation or a terrorist, also one
21 of the major ways to bring down this country is to take
22 out the electrical grid. If you take out the electrical
23 grid, you take out all communications from anybody, from
24 all your financial districts. You take out all the
25 communications the military will have. And this country

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 will come to its knees very quickly.

2 And then when you're dark like that then
3 a military attack could follow. You would be almost
4 helpless to protect yourself.

5 This next video deals with a cyber expert
6 with respect to this so-called Smart Grid that the United
7 States is trying to get on its feet. The cyber expert's
8 name is David Chalk and he discusses a threat posed by
9 Smart Merits and the Smart Grid for our national
10 security.

11 There are two sections in this video which
12 I'm going to stop and repeat because they're very
13 on-point with my petition and I want you to understand
14 these two points in respect to the entire video. This
15 guy is the foremost expert on this.

16 (Cyber Expert on Smart Grid video played.)

17 I want to repeat this one section like I
18 said I was going to do. It begins right there.

19 (Video replayed.)

20 And that's the second point I wanted to play
21 back.

22 (Video replayed.)

23 That's essentially that video on there.
24 Some of the points that I just wanted to highlight that
25 he mentioned and he's the expert was that in the public

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 domain the code is already in the public domain, the
2 codes from these corporations like Symantec and others
3 who are supposed to -- Programs are supposed to protect
4 penetration into like a nuclear power plant, into a CIA
5 computer, into a FBI computer, into a military computer.

6 The code is already there. So the hackers have a free
7 backdoor entrance into the server.

8 The other point he made there was a Trojan
9 horse and hackers have code already in the grid in
10 different servers, in different programmable logic
11 controllers and other devices at which they can activate
12 at will.

13 And then the third point, of course, is
14 there isn't anything out there that he cannot hack
15 himself that hasn't been invented. So I mean that's
16 brings it all home that everything is vulnerable
17 according to him and he's one of the foremost experts.

18 This third video I want to show is a
19 follow-through where David Chalk mentioned where a
20 diesel generator was purposely attacked and destroyed
21 using the internet. And as you watch this particular
22 video imagine an international cyber attack on emergency
23 diesel generators and put it in some 104 nuclear plants
24 in the United States.

25 (Staged Cyber Attack video played.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 That's the exhaust from the roof from that
2 generator.

3 Okay. At this time, I want to provide the
4 PRB with a brief chronology of some cyber warfare, actual
5 events. Well, not actual events, but some of the
6 chronology. There are some events in here I'm going
7 to describe later, but I want to give the chronology
8 of what this cyber warfare is all about so that you have
9 a better understanding where I'm going with related to
10 the enforcement petition.

11 Cyber warfare refers to a politically
12 motivated hacking, sabotage and espionage, a form of
13 information warfare sometimes viewed analogous to
14 conventional warfare. United States Government
15 Security Expert, Richard A. Clark, defines cyber warfare
16 as actions by a nation state to penetrate another
17 nation's computers or networks or for the purpose of
18 causing damage or disruptions.

19 In 2009, President Barack Obama declared
20 America's digital infrastructure to be a strategic
21 national asset and stated that "cyber intruders have
22 probed our electrical grids."

23 In May 2010, the Pentagon set up a new United
24 States Cyber Command and its code name U.S. CYBERCOM.
25 It's headed by General Keith B. Alexander, the Director

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of National Security Agency to defend American military
2 networks and attack other countries' systems. Notably,
3 the United States Cyber Command is only set up to protect
4 the military; whereas, the Government and the corporate
5 infrastructures are primarily the responsibility
6 respectfully of the Department of Homeland Security and
7 private companies.

8 In February 2010, top American lawmakers
9 warned that the threat of a crippling attack on
10 telecommunications and computer networks was sharply
11 on the rise. According to The Lipman Report, numerous
12 key sectors of the United States economy along with that
13 of other nations were currently at rise including cyber
14 threats to private and public facilities, banking and
15 finance, transportation, manufacturing, medical,
16 education and government, all of which now are dependent
17 on computers for daily operation.

18 The Economist writes that China has plans
19 of winning information wars by the mid 21st century.
20 They note that other countries are likewise organizing
21 for cyber war, among them Russia, Israel and North Korea.

22 Iran boasts of having the world's second largest cyber
23 army. James Gosler, a government cyber security
24 specialist, worries that the United States has a severe
25 shortage of computer security specialists, estimating

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that there are about only 1,000 qualified people in the
2 country today, but need the force of 20,000 to 30,000
3 skilled experts.

4 Military activities that use computers and
5 satellites for coordination are at risk of equipment
6 disruption. Orders and communications can be
7 intercepted or replaced. Power, water, fuel,
8 communications and transportation infrastructure all
9 may be vulnerable to disruption.

10 According to Richard A. Clark, United
11 States Government security expert, the civilian realm
12 is also at risk, noting that security breaches have
13 already gone beyond stolen credit card numbers and that
14 potential targets can also include electric power grid,
15 trains or the stock market.

16 In mid July 2010, security experts
17 discovered a malice software program called Stuxnet that
18 had infiltrated factory computers and spread to plants
19 around the world. It's considered the first attack on
20 crucial industrial infrastructure and sits at the
21 foundation of modern economies and was noted by The New
22 York Times.

23 The Federal Government of the Unites States
24 admits that the electric power transmission is
25 susceptible to cyber warfare. The Unites States

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Department of Homeland Security works with industry to
2 identify vulnerabilities and to help industry enhance
3 the security of control system networks. And the
4 Federal Government is also working to ensure that
5 security is built in as the next generation of Smart
6 Grid networks to develop.

7 However, in April 2009, reports served that
8 China and Russia had infiltrated the United States
9 electrical grid and left behind software programs that
10 could be used to disrupt the system, according to
11 current and former national security officials.

12 The North American Electric Reliability
13 Corporation has issued a public notice that warns that
14 the electrical grid is not adequately protected from
15 cyber attack. One countermeasure would be to disconnect
16 the power grid from the internet and run the net with
17 droop speed control only. Massive power outages caused
18 by a cyber attack could disrupt the economy, distract
19 from a simultaneous military attack or create a national
20 trauma.

21 Potential targets of internet sabotage
22 include all aspects of the internet from the backbones
23 of the web to internet service providers to the varying
24 types of data communication medium and network
25 equipment. This includes web servers, enterprising

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 information systems, client server systems,
2 communications links, network equipment and desktops
3 and laptops in businesses and homes. Electrical grids
4 and telecommunication systems are especially vulnerable
5 due to current trends in automation such as installation
6 of Smart Meters and applicable of the Smart Grid.

7 In February 2010, the United States Joint
8 Forces Command released a study which included a summary
9 of the threats posed by the internet which states in
10 relevant part that with very little investment and
11 cloaked in a veil of anonymity our adversaries will
12 inevitably attempt to harm our national interest.

13 Cyberspace will become a main front to both
14 irregular and traditional conflicts. Enemies in
15 cyberspace will include both states and non-states and
16 will range from the unsophisticated amateur to highly
17 trained professional hackers. Through cyberspace
18 enemies will target industry, academia, government as
19 well as military in the air, land, maritime and space
20 domains.

21 In much the same way that air power
22 transformed the battlefields of World War II, cyberspace
23 has fractured the physical barriers that shield a nation
24 from attacks on its commerce and communication. Indeed
25 adversaries have already taken advantage of computer

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 networks and the power of information technology not
2 only to plan and execute savage acts of terrorism, but
3 also to influence directly the perceptions and will of
4 the United States Government and the American
5 population.

6 Some of the more notable cyber attacks are
7 as follows. In July 2009, there were a series of
8 coordinated denial-of-service attacks against major
9 government, news media and financial websites in South
10 Korea and the United States. Well, many thought the
11 attack was directed by North Korea. One researcher
12 traced the attacks to the United Kingdom.

13 In September 2010, Iran was attacked by the
14 Stuxnet worm thought to specifically target its nuclear
15 enrichment facility. The worm is said to be the most
16 advanced piece of malware ever discovered and
17 significantly increases the profile of cyber warfare.

18 In October 2010, Lain Lobban, a director
19 of the Government Communications Headquarters, said
20 Britain faces a real incredible threat from cyber attacks
21 by hostile states and criminal and government systems
22 are targeted 1,000 times a month and that such attacks
23 threaten Britain's economic future and that some
24 countries were already using cyber assaults to put
25 pressure on other nations.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 On December 4, 2010, a group calling itself
2 Indian Cyber Army hacked the websites belonging to the
3 Pakistan Army and the others belonged to different
4 ministries including the Ministry of Foreign Affairs,
5 the Ministry of Education, Ministry of Finance, Pakistan
6 Computer Bureau, Council of Islamic Ideology, etc.

7 In July 2011, a South Korean company, SK
8 Communications, was hacked resulting in the theft of
9 personal details including the names, phone numbers,
10 home and email addresses and resident registration
11 numbers of up to 35 million people.

12 In August 2011, internet security company,
13 McAfee, reported Operation Shady RAT, an ongoing series
14 of cyber attacks which started in mid 2006.

15 On October 6, 2011, it was announced that
16 Creech Air Force Base Drone and Predator fleets command
17 and controlled data stream had been keylogged resisting
18 all attempts to reverse the exploit.

19 And at this time I'm going to put up a slide.
20 It's a August 29, 2012 Bloomberg publication
21 (<http://www.bloomberg.com/news/2012-08-29/spyware-matching-finfisher-can-take-over-iphone-and-blackberry.html>).
22 It's spyware matching FinFisher. I want to
23 discuss this document very briefly.
24

25 Here's the date, August 29, 2012.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 FinFisher spyware made by the U.K. based Gamma Group
2 can take control of a range of mobile devices. The
3 program can secretly turn on a device's microphone, track
4 its location and monitor emails, text messages and voice
5 calls.

6 FinFisher products can secretly monitor
7 computers, intercepting Skype calls, turning on web
8 cameras and recording keystrokes. When FinSpy Mobile
9 is installed on a mobile phone it can be remotely
10 controlled and monitored no matter where in the world
11 the target is located.

12 A mobile device user can become infected
13 by being tricked into going to a weblink and downloading
14 the malware which can be disguised as something other
15 than FinSpy.

16 The scanning effort led by Bill Marczak,
17 a computer science doctoral candidate at the University
18 of California Berkeley, turned up many of the same
19 machines found by Guarnieri who had used a different
20 method. It also identified new countries, bringing the
21 total number of nations with suspected command servers
22 to at least 15.

23 In one case, a sample was found transmitting
24 to the same internet address in the Czech Republic.
25 Guarnieri had identified this study as a likely FinFisher

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 command computer. It's unclear if any government
2 agencies in the countries identified in the studies are
3 Gamma clients or if the users may be based in other
4 countries.

5 So the takeaway from this article is using
6 the cell phone and this program, you know you get updates
7 all the time on your apps and whatever. I don't use
8 the cell phone that way. I'm still one of these people
9 that talk to people on these things. But it's my
10 research that there are apps you download, blah, blah,
11 blah and they send you these email links telling you
12 to update certain apps and whatnot. And that's how these
13 malware get into these SmartPhones is through these
14 updates. They're disguised as an update and they're
15 really malware.

16 And as that document states, this could be
17 anywhere in the world. So someone over there in Russia
18 could turn their cell phone on and hack someone in the
19 United States. This Fin software sets up command
20 servers like Google. The big corporation has hundreds
21 of thousands, if not millions, of servers set up all
22 over the world.

23 If they were to hack into a Google server,
24 they would have enormous power because that server,
25 they're huge. They take up acres and acres and acres.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 They have their own power plant just to power the
2 servers. So the threat is enormous and it cannot be
3 underestimated.

4 The second document I want to show you is
5 an August 30th publication. It talks about a virus
6 knocking out the computers of the Qatari gas firm. Here
7 it is. August 30, 2012. It says, "Less than two weeks
8 after 30,000 computers at the Saudi oil company fell
9 pry to a virus in Qatari's gas firm website, the corporate
10 network also down because of a virus. A hacker group
11 calling itself Cutting Sword of Justice issued a public
12 statement the day that Saudi Aramco was attacked claiming
13 it had sent a virus to destroy 30,000 computers to protest
14 Al-Saudi regime's support for government repression in
15 neighboring countries. A subsequent public message
16 from hackers indicated that Shamoon virus was used in
17 the attack."

18 Again, they're using these cell phones as
19 a means, as a weapon, to infect some major oil companies.

20 Saudi Aramco is one of the leading energy firms in the
21 world. And they wanted to destroy 30,000 of its
22 computers because of a political motivated reason.

23 I mean there are all kinds of crazy people
24 out there today and they all have their own motives.
25 And they could be a regular United States citizen who

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 attacks federal buildings. I'm sure you remember a few
2 years ago it was a United States citizen, an ex-military
3 person, in Colorado who blow up a federal building and
4 killed a lot of people.

5 Oklahoma. I'm sorry. You're right.
6 Oklahoma. My mistake. So you don't know where these
7 attacks will come from. They come from right here in
8 our homeland or they can come from across the world.
9 Cell phones are being used as a weapon. Now the
10 SmartPhones, not the cell phones. The SmartPhones.

11 All right. So now I want to talk about the
12 cyber threat to the United States in nuclear power plants
13 and other nuclear facilities via the United States
14 electric grid, the Smart Grid application and utility
15 smart meters. The Energy Policy Act of 1992 advocated
16 deregulation of electric utilities by creating wholesale
17 electric markets and required transmission line owners
18 to allow electric generation companies open access to
19 their network. With deregulation, a more complex
20 environment occurred as opposed to the traditional
21 vertically integrated monopoly that oversees the entire
22 electric grid operations.

23 Infrastructure additions which were
24 long-term planning now became an investment analysis
25 with independent power providers that decided

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 construction of new power plants under economic
2 considerations such as taxes, labor, material costs,
3 etc. and ability to obtain financing. Load and supply
4 management that fell under the midterm planning became
5 risk management as private utilities had to manage a
6 portfolio of end customers and assets with the company's
7 risk preference.

8 Many engineers argue the unfortunate
9 disadvantages that stem from deregulation where under
10 regulated monopolies, long distance energy lines were
11 used for emergencies as back-up in case of generation
12 outages. Now, particularly in North America, the
13 majority of domestic generation is sold over
14 ever-increasing distances on the wholesale market before
15 delivery to customers. This causes power grid
16 fluctuating power flows that impact system stability
17 and reliability.

18 To reduce system failure, the power flow
19 of a transmission line must operate below the
20 transmission line's capacity. Nonetheless, utility
21 companies are continually operating near capacity. As
22 utilities exchange power to other utilities, power flows
23 along all paths of the connection. And any change in
24 one point of generation and transmission affects the
25 load on all other points.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Phase and voltage fluctuation process some
2 interruptions. In sum, the economics of the electric
3 grid do not align sufficiently with the physics of the
4 grid which will ultimately cause serious consequences
5 in the near future if left unresolved.

6 Right now, I'm going to put up a slide of
7 the U.S. electric grids. I'd like to talk a little bit
8 about that. Transmission lines when connected with each
9 other become transmission networks or power grids.
10 North American has three major grids, the western
11 connection which is this area here outlined in brown,
12 the eastern connection which is over here in blue and
13 the Electric Reliability Council of Texas which is this
14 part here in green.

15 Electricity is transmitted -- Okay. So
16 looking at this particular map you have three main
17 distributions of power through transmission lines in
18 the United States on here. And I'm going to show you
19 further on an interconnection between all of these.
20 But you can see that if you disrupt this grid, it affects
21 one-third of the nation. If you disrupt this grid,
22 you're going to take down -- it's going to take down
23 another third of the nation, but you're probably going
24 to affect 80 percent of this country's ability to defend
25 itself.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Next slide, this is a typical transmission
2 system. Electricity is transmitted to high voltage 110
3 kilovolts or above to reduce energy loss to long distance
4 transmission. Power is usually transmitted through
5 overhead power lines.

6 A key limitation in the distribution of
7 electrical power is that electrical energy cannot be
8 stored and must be generated as needed. Therefore, a
9 sophisticated control system is required to ensure
10 electric generation very closely matches the demand.
11 If demand for power exceeds the supply, generation plants
12 and transmission equipment can shut down which can lead
13 to a major regional blackout such as occurred in the
14 United States Northeast blackouts of 1965, 1977, 1996,
15 2003 and 2011.

16 The discussion is this long distance the
17 longer the transmission the more power you lose. And
18 my research shows that. Once the power leaves power
19 plants through the switchyard you lose two-thirds of
20 that energy, that power, before it actually gets to the
21 customer. That's a tremendous loss.

22 This slide here shows the existing lines.
23 These are the ones -- You can't see these like light
24 green. You can see it on my computer better. It's like
25 light green here and it gets darker and darker which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is one of these arteries here, one up here and the ones
2 to the Northeast. And they are 345-499 kV, 500-699 kV,
3 700-799 kV and 1,000 kV (DC). DC is indifferent to the
4 elements which alternate for AC.

5 And then there's some proposed
6 interconnection lines where the idea is to interconnect
7 the entire continent and the United States to joining
8 all the grids together. I'm telling you a very bad idea,
9 but that's what's being proposed.

10 The next slide would be -- This slide shows
11 you existing NRC's regulation of 104 nuclear power
12 plants. These are where they are located across the
13 United States. You can see that the Northeast has more
14 than any other part of the United States. And if you
15 can in your mind think of the previous slide and show
16 the grid, imagine that electrical grids connecting
17 California over here into Washington, Virginia and you
18 have a cyber attack which takes out any portion of this
19 grid, you're going to take out the entire country. You
20 could effectively take out the entire country.

21 And when you lose outside power to the
22 nuclear power plants, of course, emergency diesel
23 generators have to come on and pick up the task for the
24 nuclear fuel. We saw what happened to those diesel
25 generators when they were hacked in by a cell phone.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The next slide. This one is the Bloomberg
2 news article and it talks about the group I previously
3 mentioned called the Comment Group
4 (<http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html>)
5 1). The date should be on this thing. Here's the date
6 right there. It's July 26, 2012. Hackers
7 clocked in at precisely 9:23 a.m. Brussels time on July
8 18th last year and set to their task in just 14 minutes
9 of quick keyboard work. They scooped up the emails of
10 the president of the European Union Council, Herman Van
11 Rompuy, Europe's point man for shepherding the delicate
12 politics of the bailout for Greece according to a
13 computer record of the hacker's activity.

15 Over ten days last July hackers returned
16 to the Council's computer four times accessing internal
17 communications of 11 of the EU's economic, security and
18 foreign affairs officials. The breach unreported until
19 now potentially gave the intruders unvarnished view of
20 the financial crisis ripping Europe.

21 The research has identified 20 victims in
22 all, many of them organizations with secrets that could
23 give China an edge as it strives to become the world's
24 largest economy. The targets included lawyers pursuing
25 trade claims against the country's exports and an energy

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 company preparing to drill in the waters China claims
2 as its own.

3 What the general public hears about stolen
4 credit card numbers someone hacked, that's the tip of
5 the iceberg. The unclassified stuff, said Shawn Henry,
6 former Executive Assistant Director of the FBI in charge
7 of the agency's cyber division until leaving earlier
8 this year. I've been circling the iceberg in a
9 submarine. This is the biggest vacuuming up of United
10 States propriety data that we've ever seen. It's a
11 machine.

12 The methods behind China-based alluding of
13 technology and data and most of the victims have remained
14 for more than a decade in a murky world of hackers and
15 spies fully known in the United States only to a small
16 community of investigators with classified clearances.

17 Until we can have this conversation in a transparent
18 way, we're going to be hard-pressed to resolve the
19 problem, said Amit Yoran, former National Cyber Security
20 Division Director at the Department of Homeland
21 Security.

22 Yoran now works for RSA Security Inc., a
23 Bedford, Massachusetts based security company which was
24 hacked by the Chinese teams last year. I'm just not
25 sure America is ready for that, he said.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 What has started as assaults on military
2 and defense contractors has widened into a rash of
3 attacks from which no corporate entity is safe, say U.S.
4 Intelligence officials who are raising the alarm in an
5 increasing dire terms.

6 Private researchers have identified 10 to
7 20 Chinese hacking groups that said very significantly
8 in activity and size. What sets the Comment Group apart
9 is a frenetic pace of its operations. The attacks
10 documented last summer represent a fragment of the
11 Comment Group's conquests which stretch back to at least
12 2002 according to incident reports and interviews of
13 investigators.

14 Milpitas, a California-based FireEye,
15 Inc., alone has tracked hundreds of victims in the last
16 three years and estimates the group has hacked more than
17 1,000 organizations, said Alex Lanstein, a senior
18 security researcher. Stolen information is flowing out
19 of networks of law firms, investment banks, oil
20 companies, drug makers, high technology manufacturers
21 in such significant quantities that intelligence
22 officials now say it could cause long-term harm to the
23 United States and European economies.

24 One Comment Group trademark involves
25 hijacking unassuming public websites to send commands

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 to victim computers, turning mom-and-pop sites into
2 tools of foreign espionage, but also allowing the group
3 to be monitored if those websites can be found, according
4 to security experts. Sites it has commandeered include
5 (1) for a teacher in South Texas high school with a
6 website motto of "Computers Rock!" and another for "Drag
7 Racing, Track Outside Boise, Idaho."

8 Others not publicly attributed to the group
9 before include a campaign against North American natural
10 gas producers that began in December 2011. And that
11 was detailed in an April alert by the Department of
12 Homeland Security, two experts who analyzed the attack
13 said.

14 In another case, the hackers first stole
15 a contact list for subcontractors to a nuclear management
16 newsletter and then sent forged emails laden with
17 spyware. In that instance, the group succeeded in
18 breaking into a computer network of at least one
19 facility, Diablo Canyon Nuclear Plant, next to the Hosgri
20 fault north of Santa Barbara, according to a person
21 familiar with the case who asked not to be named.

22 Last August the plant's incident management
23 team saw an anonymous internet post that had been making
24 the rounds among cyber security professionals. They
25 purported to identify web domains being used a Chinese

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 hacking group including one that suggested a possible
2 connection to Diablo plant operator Pacific Gas &
3 Electric Company, according to an internal report
4 obtained by Bloomberg News.

5 It's unclear how the information got to the
6 internet, but when the plant investigated it found that
7 the computer of a senior nuclear planner was at least
8 partially under the control of hackers, according to
9 the report. The internal probe warned that the hackers
10 were attempting to identify the operations,
11 organizations and security of the United States nuclear
12 power generating facilities.

13 Around the time the hackers were sending
14 malware-laden emails to the United States nuclear
15 facilities, six people at the Wiley Rein law firm were
16 ushered into a hastily called meeting. In the room were
17 an ethics compliance officer and a person from the firm's
18 information technology team, according to a person
19 familiar with the investigation. The firm had been
20 hacked, each of the six were told and they were the
21 targets.

22 In case after case, the hackers had the run
23 of networks they were rifling. It's unclear how many
24 of the organizations researchers contacted. The trail
25 last summer led to some unlikely spots including

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Pietro's, an Italian restaurant a couple blocks from
2 Grand Central Station in New York. The Comment Group
3 stopped using the restaurant site to communicate with
4 hack networks sometime last year, said FireEye's
5 Lanstain who discovered that the hackers had left
6 footprints there. Traces are still there.

7 Hidden in a webpage code of the restaurant's
8 site is a simple command, ugs 12, he said. It's an order
9 to captive the computer on some victim's network to steep
10 for 12 minutes and check back in, he explained. The
11 ug stands for ugly gorilla which security experts believe
12 is a moniker for a particularly brash member of Comment,
13 a signal for anyone looking that the hackers were there,
14 said Lanstein.

15 So this actually formed the basis of my
16 authorizing the 2.206 Petition requesting NRC to take
17 enforcement action in this case. As you can see from
18 this article which has been demonstrated from the
19 presentation itself so far, these hackers, they
20 commandeer anybody's server. It could be a school.
21 It could be a library. It could be a hospital. It could
22 be a restaurant in New York City.

23 And from that server that becomes their
24 command operation to launch attacks to the cyberspace,
25 the internet. And in this case, Diablo Canyon Nuclear

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Power Plant, it was apparently breached.

2 And according to this article they were
3 looking for information of how to gain access to other
4 nuclear power plants that are under the control and
5 regulation of the Nuclear Regulatory Commission.

6 This last video I'm going to show is a video
7 from the Homeland Security Department itself. It was
8 made on July 4th of this year, 2012. It's the most recent
9 that I have.

10 (CNN Homeland Security video played.)

11 So the point that I take away from this is
12 that the Nuclear Homeland Security has already
13 documented that nuclear facilities have been breached
14 in more than one way. But particularly interesting was
15 that this news broadcast talked about a jump drive, a
16 USB drive, that you just plug into your computer.

17 So managers all the time do work at home
18 on their computers, save their files to their USB jump
19 drive or USB stick, whatever you want to call it. And
20 they take it to work and make presentations. So there's
21 more than ample opportunity for a malware to have
22 infected their presentation through that jump drive.
23 And now that jump drive has unescorted access to any
24 nuclear power plant simply by being taken in by someone
25 who has unescorted access to a nuclear power plant.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 From that point in it can infect the servers of the
2 utility and spread through the internet to all servers,
3 even NRC servers, here at your headquarters.

4 So I briefly talk about 10 CFR 73.54 and
5 certainly the licensee's response to the NRC's data
6 request should include how they would address that
7 threat, someone bringing in either a CD, stick or I think
8 they still make the hard disks, although they might be
9 hard to find. The floppy disks I think they call them.

10 So if you bring that type of information into your
11 nuclear power plant, how is that going to be controlled?

12 It would be very difficult I think.

13 This last slide I'm going to -- next to the
14 last slide, I want to put up here is here's a website.

15 It's called www.backtrack-linux.org. You can pull
16 this up on the web at your leisure. But this is the
17 latest rev. It's called BackTrack 5 R3, August 13, 2012.

18 Now I'm not the smartest kid on the block
19 when it comes to computers, but I downloaded this
20 software. It's an ISO file. And if you burn that to
21 a CD and then you reboot your computer, what happens
22 is that Linux -- it's a Linux operating system versus
23 Microsoft operating system -- places itself -- becomes
24 your operating system of your computer for that
25 particular program.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And that program will allow you -- I can
2 do it here briefly. Like this is my link here for
3 internet. So here's all the available WiFi available
4 links I can hook up to the internet. I can go to this
5 Verizon which is secure. This AMX, it says right here,
6 it's insecure. So I can get on here without a password
7 or any type of security code.

8 And here's one with WPA2-PSK security.
9 That's the most recent, most effective security software
10 to prevent you from taking my computer and being able
11 to access my accounts over the internet and breaking
12 into my internet connection. That's the best that we
13 have right now.

14 And just the list goes on depending on where
15 you're at. So if you were adjacent to a nuclear power
16 plant and they were connected to the internet and if
17 they had someone had WiFi internet access, you could
18 break into their server this way.

19 This software when you load this up it will
20 pull up all those access points I just showed you. And
21 it will religiously work forever until you turn your
22 computer off. And it will break that access. It will
23 show you the user's name and their password. And this
24 is a run-of-the-mill computer. It's a used computer,
25 but I think it's a quad-core microprocessor. It's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 pretty fast. It's like 3 gigahertz. And it works.

2 I'm not a computer expert. I could break
3 in. I could go to anywhere. I could go out in the
4 parking lot, pick up the signal and break in using this
5 software and find out the user's name and passcode
6 relatively quickly. If you've got a very sophisticated
7 passcode it might take a week or two weeks. But this
8 program will break it. And this is public domain.
9 Anybody gets this for free.

10 Like that expert, Mr. Chalk, talked about,
11 if it's out there, he can hack it and he can. And he's
12 talking about the SmartGrid and the SmartMeters which
13 I'm going to get into now very quickly here.

14 So I'm trying to link the 2.206 petition
15 to these threats posed by the electrical grid of the
16 United States and SmartMeters and their application
17 which goes far beyond a customer location as you will
18 see very shortly. To do that I'm going to pull up this
19 last article.

20 This is a Florida Power & Light Company
21 document. It's a case study. Florida Power & Light
22 -- it might seem like I'm picking on them, but I just
23 happen to have this document because I'm involved in
24 one of their rate cases. So I have a lot of research
25 on them right now.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 But this is atypical of all utilities across
2 the United States right now who are involved in SmartGrid
3 applications. Florida Power & Light or FPL has 4.6
4 million customers, nearly 70,000 miles of power lines
5 and 16 power plants. Florida Power & Light Company is
6 one of the nation's largest electric utilities. Their
7 parent company is NextEra Energy. And they've got
8 nuclear facilities across the United States and wind
9 generation and natural gas.

10 And it doesn't matter if it's wind
11 generation or natural gas. I mean if it's wind
12 generation you take down and it's tied to the grid, you've
13 got access to the country's entire grid. So any access
14 point. It doesn't have to be a nuclear power plant.

15 FPL SmartGrid plan involve a deliberate and
16 phased approach to date. Equipment is installed and
17 operational for about 98 percent of the project's planned
18 transmission system improvement, 50 percent of the
19 planned distribution system improvements and 75 percent
20 of the planned SmartMeter changeout. As of April 2012
21 FPL installed more than 5,000 intelligent monitors,
22 sensors and controls on their transmission and
23 distribution grid.

24 Smart devices have been installed in 78
25 substation transformer banks. The installation effort

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 included replacing about 50 electro-mechanical
2 protective relay systems with state-of-the-art
3 computer-based systems and installed feeder, breaker
4 and regulator intelligent electronic devices at nearly
5 100 substations, more than 200 automatic feeder switches
6 and 45 phaser measurement units.

7 FPL's upgraded Transmission Performance
8 and Diagnostic Center remotely monitors power
9 transformers in 500 FPL substations. In January 2012,
10 a newly installed monitor detected an out-of-phase
11 tolerance high voltage bushing. Customers served by
12 this transformer were temporarily switched to another
13 one. And the affected transformer was removed from
14 service.

15 The TPDC is also monitoring the battery
16 banks that provide power to 500 FPL substations. The
17 battery banks are monitored for both high voltage and
18 low voltage levels and high impedance. The TPDC is also
19 monitoring the capacity of voltage transformers and is
20 measuring voltage levels and other power flow variables.

21 FPL plans to build on its SGIG-enabled
22 SmartGrid capabilities for future products, services
23 and applications. We are conducting pilot projects to
24 learn how the SmartMeters work with other components
25 on the system. FPL along with other electric utilities

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 around the country have been given hundreds of millions
2 of dollars in grants from the United States Government
3 to promote SmartGrid applications.

4 And this chart here if you have a SmartMeter
5 and you're an FPL customer you can go to the internet,
6 pull up your account with FPL by typing in your user
7 name and password. And you click on the history usage
8 and all it does is show you how much power you're using
9 at any particular day in any particular hour of the day.

10 And by some magic this utility thinks customers are
11 going to save money because they can see this.

12 You know, first of all, anybody with half
13 a brain could walk to a meter and read the kilowatt hours
14 off their meters right now. The majority of the meters
15 are digital. So it's going to give you the actual
16 kilowatts hours you're charged. You're charged by
17 kilowatt hours of electricity by all utilities. One
18 thousand watts of electricity. They've got
19 kilowatt-hours like 9.5 cents right now. So the bill
20 is going to be \$95.

21 If you go over 1,000 kilowatts, you get
22 penalized because you're getting into a higher rate.
23 The Utility Commission of Florida allows them to charge
24 a higher rate. So the idea is to keep everybody under
25 1,000 kilowatts hours and you'll have the lowest bill

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 reasonably achievable.

2 What FPL did and again I'm not picking
3 on them. I'm just giving you because of my research
4 in the rate case. What they did is they put these
5 SmartMeters in. They didn't ask anybody if they wanted
6 one. They just went on their property, took the analog
7 meter out, slapped the SmartMeter in there and said,
8 "Have a good day" while everybody is revolting on this.

9 Like 8,000 were moved already, but they
10 didn't want them on their property because first of all
11 it's the wrong meter. The customers are getting yanked
12 around twice. We pay taxes to the government. The
13 government gave FPL this money. Now FPL is charging
14 us to use that money to put a SmartMeter which we don't
15 really want.

16 But the meter is the wrong meter because
17 when I say that the meters they're putting in are
18 SmartMeters. But they don't have the capability of
19 common use.

20 Also for the SmartMeter to be applicable
21 the way the government intended in order to work is that
22 the meter has to be able to communicate with your
23 appliances. You have to have smart appliances. You
24 have to have a refrigerator, electric range, a
25 dishwasher, a washing machine and dryer that have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 microprocessors in them so the SmartMeter can tell them
2 when to turn on and off. The idea being when big business
3 comes on line they're pulling all these megawatts of
4 power that there are certain times a day this occurs.

5 And those peak times, if they can have the
6 customers agree to allow them to control their appliances
7 in their house during these peak times, then FPL says
8 "We'll give you a lower price on your electric." And
9 they become a public service commission. "This will
10 help us not build more power plants because we won't
11 have to increase our capacity to meet the peak load."

12 In reality, they have put a bunch of meters
13 in to millions of customers that don't meet those
14 requirements. So they're useless. And people have
15 concerns about the RF radiation coming from them. They
16 have concerns FPL having access to what they're using
17 and how much electricity and what time.

18 Anyway, there's a big debate going on about
19 that. But the issue here and why this is relevant to
20 the Petition is that these are, as Mr. Chalk has
21 described, access points to nuclear power plants and
22 nuclear facilities like reprocessing plants and fuel
23 processing plants and even plants that make fuel rods.

24 I used to work at a Westinghouse facility
25 that made fuel rods. And they all went internet

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 connections. So anyway you can get into the internet
2 through a SmartMeter, using a phone or a computer or
3 a software program. Then you have access to a nuclear
4 power plant.

5 What's relevant on this document, what's
6 really alarming on this document, is this is just one
7 utility. This is going on all over the country.
8 Ninety-eight percent transmission system improvements.

9 And if they have the Smart devices, these devices that
10 are computer controlled remotely, to cause switching
11 functions at their substations so that they can control
12 power back to a service area that is down for one reason
13 or another.

14 But in the hands of a terrorist, they're
15 going to look at them and said, "My God, we can control
16 500 FPL transformers now, switching transformers."
17 Five thousand intelligent monitors, sensors and controls
18 on their transmission and distribution grid. Seventy
19 thousand miles of grid. FPL is connected to the
20 Northeast grid.

21 So if you take down the State of Florida
22 which the high voltage lines go right to the end of the
23 tip of Florida into Georgia you're going to take down
24 the entire Northeast United States. And if eventually
25 the government decides to interconnect all three major

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 grids you can take down the entire country just by taking
2 down any part of that grid. It's a very dangerous and
3 tenuous situation.

4 If terrorists were to infiltrate a nuclear
5 power plant in Florida -- for example, we've already
6 seen where they've attempted it at Diablo Canyon -- let's
7 just look at Florida. If they were to access the same
8 St. Lucie nuclear power plant and cause the off-site
9 to lose offsite power and at the same time they attack
10 Turkey Point causing it to lose offsite power through
11 these Smart devices, and the Crystal River nuclear plant
12 on the west coast and they did the same thing. So you
13 have five nuclear power plants that have no offsite
14 power. Emergency diesel generators start.

15 Well, they hack into the emergency diesel
16 generators and they blow every one of those up. So now
17 you've got five nuclear power plants with no way to keep
18 the reactor core cool. Within an hour or less, those
19 cores are all going to be melting down and depends on
20 the specifications they could attack the power for the
21 fuel pools. So you're going to have those go critical
22 because there's no cooling wire to keep the spent fuel
23 cool.

24 Now you have five nuclear reactors that are
25 melting down simultaneously. And you've got these five

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 nuclear fuel pools melting down simultaneously. You
2 cannot stop that type of event. They're going to melt
3 down just like Fukushima did no matter what you try to
4 do.

5 And that's a big threat in my mind. I'm
6 not posing to be an expert. But just on the basis of
7 all the information the United States Government has
8 put together over the years and all the experts that
9 will have knowledge of these things, that's a real
10 incredible threat. And it's not being dealt with by
11 anybody right now.

12 Now again at the beginning of this meeting
13 I asked that the NRC think outside the box. Being outside
14 the regulations of your regulations you have to. That's
15 what needed to be done on 9/11. 9/11 as tragic as that
16 incident was, you take down the United States electric
17 grid and you're going to have -- that incident will pale
18 in comparison to the tragedy that will happen if you take
19 down the electric grid.

20 It will involve all communications. The
21 financial markets will go into chaos. All the banks will
22 be kaput. The military will be down because they won't
23 be able to communicate with each other. And I mean the
24 country is wide open for a full military attack at that
25 point. You won't be able to defend yourself.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 In the midst of all this, this country has
2 a dysfunctional United State Congress who doesn't want
3 to address and resolve a terrorist bill, a cyber warfare
4 terrorist bill. And that's an issue beyond the scope
5 of this Commission. But you still have to understand
6 that is overhang of all of this.

7 And you have a financial crisis. This
8 country is almost \$17 trillion in debt. And no one wants
9 to address that problem realistically.

10 So the point is in my view as a citizen of
11 this country this country right now as we sit here today
12 is at its most vulnerable point ever because you have
13 a financial crisis going on. You have a dysfunctional
14 Congress. And we don't know who is going to be the next
15 President of the United States.

16 And we have a situation here which could
17 bring down the entire electric grid of the United States
18 and affect all 104 United States nuclear power plants.

19 And Al Qaeda has religiously attacked. And so they could
20 take out each grid. They could plan an attack on each
21 grid and take out all three grids at the same time.

22 And I've personally worked at Palo Verde
23 Nuclear Power Plant and on occasions I wandered out into
24 the desert because I've never been in a desert before.

25 And here I was standing under the transmission lines

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and that was the desert.

2 And it's very hot out there. So the lines
3 were drooping. They were only like only 20, maybe 30,
4 feet above my head. I could have thrown a chain across
5 them and took out the entire grid if I wanted to. Or
6 I could have plants some C-4 along the tower.

7 There was nobody within thousands of miles of me.

8 No one even knew I was there. You could almost hear
9 your heartbeat it was so quiet. You could take down the
10 transmission tower. One person could take down an entire
11 grid, that whole section, I showed you on the chart just
12 by taking down that transmission grid. So systems are
13 very vulnerable.

14 These SmartMeters, you know, the NRC has
15 authority over its licensees. And under these
16 regulations that you have -- maybe you need to make some
17 new ones -- I don't know. But you need to adjust the
18 SmartMeters. The SmartMeters need to go away. And it
19 just can't be from the public pushing to have them
20 removed.

21 Not only the SmartMeters on the commercial
22 businesses and the residential homes. The SmartMeter
23 applications like FPL putting out here on their
24 transformer banks and on their grid, those have to go
25 away. You cannot allow remote access.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And I've heard the expert. Even though how
2 well you think you're protecting it, he can hack into
3 it. And he'll do it on national TV. This guy is like
4 the best of the best.

5 We're vulnerable. And I don't know how far
6 along other utilities are with this SmartGrid application
7 and stuff, but that needs to be nipped in the bud right
8 now.

9 And beyond that inside your nuclear power
10 plants you have programmable logic controllers and your
11 IST expert can tell you about that. And if you hack in
12 -- If you're gain access to nuclear power plants, a
13 programmable logic controller is a mini-computer all by
14 itself. And it has a program in it to make certain
15 equipment operate within certain parameters. And you
16 can alter each individual program. And if you put a virus
17 in a nuclear power plant it can just go haywire. You
18 can be in serious trouble very quickly.

19 The Petition asks -- what I'm looking for
20 in this Petition is really you need to isolate all the
21 nuclear plants in the internet. And it has to be
22 completely isolated. There is no need for a nuclear power
23 plant to have internet access in my view.

24 We've operated them for years without
25 internet access when they were first constructed. They

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 don't need internet access now to operate under their
2 licenses. And there's just got to be some kind of
3 policies and procedures put in place.

4 You can't bring jump drives in and make your
5 presentations from them. And even though they're
6 scanned, I'm telling you that there is sophisticated code
7 that will not be detected by all malware programs like
8 Symantec puts out and Norton and all these. There are
9 programs beyond the scope of those and they will not be
10 detected. So you can get a virus in even though your
11 licensee software may say it's safe to run that program.

12 It can still be infected.

13 And the real problem -- You know one of the
14 major concerns I have is this guy is saying that the codes
15 are already in the grid, the malware. And it can be
16 activated at any time. So that's the more reason to
17 isolate the nuclear power plants so that the generators,
18 the diesel generators, can come on when they're called
19 to and meet the cooling needs of the reactor core and
20 spent fuel pools.

21 Otherwise you're going to have a catastrophe
22 that we'll never recover from. You can contemplate the
23 entire country if all 104 nuclear reactors melt down in
24 a reasonably same period of time.

25 And at that that's about all I have. And

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I'll be glad to answer any questions anybody has.

2 CHAIRMAN NIEH: Okay. Thank you, Mr.
3 Saporito. At this time, I think we'll transition to
4 any questions or clarification for understanding from
5 the NRC staff. Again, I'd like to remind the NRC folks.
6 This is public meeting. So let's not discuss any
7 security, safety-related or safeguards information.

8 I'll open it up to the NRC staff that are
9 in the room here from the Petition Review Board. Please.

10 MR. PEDERSON: Perry Pederson, NRC Cyber
11 Security Specialist. At this point, I just have one
12 question. You mentioned that the NRC regulation 10 CFR
13 73.54 doesn't go far enough. And I'm sure you've read
14 it. It's only two pages long.

15 And the statement in there, it's
16 characterized as "the licensees are required to provide
17 high assurance against a cyber attack." And, of course,
18 you've probably also read our regulation. If you
19 haven't, I hope you will.

20 But you said that doesn't go far enough.
21 I wondered if there was something beyond what you've
22 already stated in the Petition. How would you
23 characterize what far enough is?

24 MR. SAPORITO: Well, you mentioned the words
25 "reasonable assurance."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. PEDERSON: No, "high assurance."

2 MR. SAPORITO: Okay. "High assurance."
3 You need in my view "positive assurance." You need
4 "absolute assurance." And the only way you're going to
5 get that is you have to make sure that the licensees are
6 not -- their nuclear power plants are not -- allowed to
7 access the internet. There is no internet access.

8 Otherwise, someone is going to access the
9 internet. Is going to potentially infiltrate their
10 system and either destroy equipment, cause a reactor to
11 melt down, destroy the nuclear spent fuel pools. The
12 only way -- You can't get -- I mean you can write as many
13 policies. The licensee can proffer as many policies and
14 procedures as they want to you, but they are only pieces
15 of paper.

16 And what you have in reality at these
17 licensed facilities is human beings. People are going
18 to bring jump drivers into work. Maybe we've had nuclear
19 reactor operators goofing off on the internet while
20 they're supposed to be running the nuclear reactor.

21 It's human nature. You can't -- You know
22 people aren't machines. So they're going to do the wrong
23 thing at the wrong time.

24 The only way to -- This is so serious that
25 you have to actually -- Like I say, I'm not proffering

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 rulemaking here, but there has to be a requirement, a
2 regulation. It can't be an expectation. It's got to
3 be like a regulation or a requirement of no internet
4 access.

5 There is no reason for a nuclear power plant
6 to access the internet in my view. They run fine without
7 internet access. I mean that's the only credible way.

8 If you don't want the computer internet, take the Cat
9 5 cable out of the computer. Now you're not on the
10 internet. You have to disconnect the nuclear power plant
11 from the internet. That's the only failsafe way to do
12 that in my view.

13 CHAIRMAN NIEH: Okay. Are there any other
14 questions from the PRB members?

15 MR. MOSSMAN: On video number 3 was the
16 Homeland Security video. It's the staged cyber attack
17 on a diesel generator. You had later mentioned that that
18 was -- I don't know if I just didn't hear you correctly,
19 but you had mentioned something about that being initiated
20 from a SmartPhone.

21 I don't know that I saw that on the video.

22 So I wasn't sure what the connection there was between
23 the SmartPhone and the diesel attack.

24 MR. SAPORITO: It's my understanding that
25 the nuclear attack was launched by a research group from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 a university to prove that it could be done over the
2 internet. I don't know if they used a SmartPhone or a
3 computer or whatnot, for certain how they did it. But
4 they did it. They did do it.

5 CHAIRMAN NIEH: Okay. This is Ho Nieh. I
6 did have a couple questions. Thank you for your
7 presentation.

8 This came up in one of the videos and again
9 in some of your commentary in presenting the information.

10 Do you have any specific evidence or any other detail
11 related to how or whether or not cell phones can be used
12 to access a nuclear power plant's control systems?

13 MR. SAPORITO: Well, just like the experts
14 testified, if you can get access from a SmartPhone to
15 a SmartMeter or any application on the SmartGrid, you
16 really don't need to get inside the power plant. All
17 you need to do is take off offsite power and you're going
18 to cause a situation where the diesel generators have
19 to pick up the cooling loads.

20 And then at that point if you can get access
21 to the nuclear power plant through the internet you can
22 take out the emergency diesel generators and then the
23 ballgame is over after that.

24 CHAIRMAN NIEH: Okay. So it's from the
25 expert testimony that was presented.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. SAPORITO: Yes. I have no -- I haven't
2 developed any program that can do it.

3 CHAIRMAN NIEH: Okay.

4 MR. SAPORITO: It's well beyond my
5 capabilities.

6 CHAIRMAN NIEH: Okay. I did have a question
7 similar to the diesel generator one that Peter asked as
8 well. I guess toward the end you talked about NextEra
9 and Florida Power & Light. Were there specific concerns
10 with any Florida Power & Light facilities? Or is this
11 just really laying out the potential threat of losing
12 the entire grid with these SmartGrid improvements?

13 MR. SAPORITO: It's more of a layered
14 concern. Primarily you have Florida Power & Light with
15 this aggressive SmartGrid/SmartMeter program which the
16 document shows how advanced it is. And that's putting
17 the Turkey Point/St. Lucie nuclear facilities at risk
18 immediately in my view because all of these SmartMeters
19 are already installed which can be accessed through the
20 internet.

21 But the concern is even more tenable because
22 all the transformers that have devices that can be hacked
23 into over the internet. Their substations and their
24 battery banks and their switchyards, it's enormous. And
25 it's put on this fast track.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 They've got money and they want to get more
2 money from the PSC. And they want to have all these
3 SmartMeters put on the residential customers and all the
4 businesses. It's interconnected with Crystal
5 River because they share a common grid.

6 If you have a situation where you're attacked
7 on FPL's grid, you're actually attacking the entire grid
8 of Florida which is interconnected with the Northeastern
9 grid. So you're essentially attacking the heart of the
10 United States. If you lose the Northeastern grid, you're
11 in very serious trouble.

12 CHAIRMAN NIEH: Okay. And my last question
13 related to your petition. Is your focus for these
14 enforcement actions limited to commercial power reactors
15 licensed by the NRC?

16 MR. SAPORITO: No. I think the petition
17 speaks to all NRC licensees. If you have a nuclear fuel
18 reprocessing facility or a facility that makes nuclear
19 fuel or a facility that makes fuel rods, hospitals that
20 have radiophotography and whatnot, all those licensees
21 could be attacked somehow through the internet.

22 And you don't have to have a conventional
23 bomb to explode to harm people. You could have a dirty
24 bomb made from the waste from a hospital. And if they
25 could get access by hacking into the security of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 hospital to gain access to that material, there you go.

2 So it's a very pervasive problem.

3 CHAIRMAN NIEH: Okay. Thank you.

4 Any other questions from the NRC staff in
5 the room here?

6 (No verbal response.)

7 How about NRC staff that are on the phone?

8 Any questions for Mr. Saporito?

9 (No verbal response.)

10 Okay. Hearing none, I'd like to move on to
11 any licensees that are present in the room today. Do
12 you have any questions for Mr. Saporito?

13 (No verbal response.)

14 Any licensees on the phone that have any
15 questions for Mr. Saporito?

16 (No verbal response.)

17 Okay. Let's see here. Okay. I think that
18 concludes your presentation, the staff's questions and
19 the licensees' questions for clarification. And before
20 I conclude the meeting, I'd ask if there are any other
21 members of the public in this room that have any questions
22 about the NRC's 2.206 process.

23 (No verbal response.)

24 No. Okay. Mr. Saporito, thank you for
25 taking the time to present the details of your petition.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I thought the information you presented was helpful and
2 it helped us better understand the petition that you
3 submitted to the NRC for review.

4 Court Reporter, do you have any questions
5 for clarification that you need at all?

6 COURT REPORTER: I have a few questions
7 which I can ask off the record.

8 CHAIRMAN NIEH: Okay. That will be fine.

9 Hearing nothing else, then that concludes
10 our public meeting for your 2.206 Petition. Thank you.

11 MR. SAPORITO: Is there any public on the
12 line?

13 CHAIRMAN NIEH: I didn't know if we had any.

14 MS. MENSAH: They're not required to
15 introduce themselves and no one did. Did we unmute the
16 lines for the licensees to respond?

17 CHAIRMAN NIEH: Yeah. I didn't ask that.
18 I didn't realize they were on mute though.

19 MS. MENSAH: Just ask that.

20 CHAIRMAN NIEH: Is the Headquarters
21 Operations Center there? Is the HOO on the line?

22 (No verbal response.)

23 OPERATOR: Yes.

24 CHAIRMAN NIEH: Yes. This is Ho Nieh, the
25 Petition Review Board Chair. I forgot to ask to have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the phone lines unmuted so that any of the licensee
2 participants or any other parties that joined the bridge
3 could ask any questions. Could you unmute the line?

4 OPERATOR: I'm unmuting the line now.

5 CHAIRMAN NIEH: Okay. Let me know when
6 that's done.

7 OPERATOR: Headquarters OPs officer. The
8 line is unmuted.

9 CHAIRMAN NIEH: Thank you. Hi. This is Ho
10 Nieh, the Petition Review Board Chair. My apologies.
11 I forgot to have the phone lines unmuted. I did want
12 to go around to see if any licensees that are on the line
13 have any questions for Mr. Saporito.

14 (No verbal response.)

15 That sounds silent to me. Are there any
16 other members of the public that may have joined the
17 teleconference bridge on the line?

18 (No verbal response.)

19 Okay. I'm not hearing a response. So with
20 that I'll conclude the meeting. Thank you for your
21 presentation. Off the record.

22 (Whereupon, at 1:52 p.m., the above entitled
23 matter was concluded.)

24

25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1
2
3
4
5
6
7
8
9
10
11
12

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com