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

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/ORA

TIM MOSSMAN, NRR/DE/EICB

PERRY PEDERSON, NSIR/DSP/ISCPB

NICOLE COLEMAN, OE (Advisor)

CARRIE SAFFORD, OGC (Advisor)

NRC HEADQUARTERS STAFF PRESENT:

RONALD ALBERT, NSIR/DSO/RSDB

JOE DEUCHER, NSIR/DSP/CSIRB

MARK LOMBARD, NMSS/SFST

DAVID PELTON, NRR/DPR/PGCB

BLAKE PURNELL, NRR/DPR

ANDREA RUSSELL, NRR/DPR/PGCB

ALEX SAPOUNTZIS, NSIR/DSP/FCTSB

ALSO PRESENT:

MATT DELLON, Pacific Gas & Electric*

STEVEN HAMRICK, FPL*

JEFF LeCLAIR, Xcel Energy*

DAVID REPKA, Winston & Strawn/Pacific Gas & Electric

CRAIG ROSEN, Pacific Gas & Electric*

JAMES ROSS, GE Hitachi

*Participating via teleconference

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

P R O C E E D I N G S

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

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

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

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

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

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

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

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

For those here in the room, please speak up so that those on the phone can hear clearly and so that the court reporter can accurately record your name. I will start with myself and the other NRC participants

here in the room.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. ROSS: James Ross, GE Hitachi.

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

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

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

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

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

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

(Roster playback.)

Is the NRC Operations Center on the line?

MR. LeCLAIR: Jeff LeClair with Xcel Energy.

MR. HAMRICK: Steve Hamrick, NextEra Energy.

MR. ROSEN: Craig Rosen and Matt Dellon,

Pacific Gas & Electric.

(Roster playback complete.)

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

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

MS. MENSAH: Thank you.

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

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

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

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

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

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

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

CHAIRMAN NIEH: I sure can. Okay.

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

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

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

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

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

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

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

In addition, we are also coordinating with several other NRC offices with representatives from the Office of Federal and State Materials and Environmental Management Programs, the Office of Nuclear Material Safety and Safeguards and the Office of New Reactors. And we have these offices involved to take a look at whether your petition affects or relates to any other NRC licensed facilities outside of power reactors.

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

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

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

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

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

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

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

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

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

As I mentioned, on July 30th, the Petition

was submitted.

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

On August 27th, the Petition Review Board members and advisors met to discuss the Petitioner's request for immediate action. And though an immediate action wasn't explicitly called out for in the Petition, we treated your request as if it were in immediate action. And we looked as far as an immediate action goes whether it should be required that all NRC licensees take their nuclear reactors and/or facilities to a cold shutdown mode of operation as described in the Petition.

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

(1) safety related and important to safety functions;

(2) security functions;

(3) emergency preparedness; and

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

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

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

I also want to mention that the NRC staff

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

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

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

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

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

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

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

across the United States.

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

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

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

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

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

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

Well, things have changed since that time. We used to leave our -- You know, people left their doors open in their homes. They felt safe and secure. And now you don't do that anymore.

And then you invented this thing called the cell phone. People don't use it to talk to each other. They would rather text and send emails and get on the internet and all that kind of good stuff I guess that is.

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

And this is one of the reasons again that

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

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

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

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

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

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

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

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

(Cyber Shockwave video played.)

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

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

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

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

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

will come to its knees very quickly.

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

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

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

(Cyber Expert on Smart Grid video played.)

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

(Video replayed.)

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

(Video replayed.)

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

domain the code is already in the public domain, the codes from these corporations like Symantec and others who are supposed to -- Programs are supposed to protect penetration into like a nuclear power plant, into a CIA computer, into a FBI computer, into a military computer. The code is already there. So the hackers have a free backdoor entrance into the server.

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

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

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

(Staged Cyber Attack video played.)

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

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

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

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

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

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

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

The Economist writes that China has plans of winning information wars by the mid 21st century. They note that other countries are likewise organizing for cyber war, among them Russia, Israel and North Korea. Iran boasts of having the world's second largest cyber army. James Gosler, a government cyber security specialist, worries that the United States has a severe shortage of computer security specialists, estimating

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Here's the date, August 29, 2012.

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

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

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

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

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

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

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

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

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

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

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

Again, they're using these cell phones as a means, as a weapon, to infect some major oil companies. Saudi Aramco is one of the leading energy firms in the world. And they wanted to destroy 30,000 of its computers because of a political motivated reason.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The methods behind China-based alluding of technology and data and most of the victims have remained for more than a decade in a murky world of hackers and spies fully known in the United States only to a small community of investigators with classified clearances. Until we can have this conversation in a transparent way, we're going to be hard-pressed to resolve the problem, said Amit Yoran, former National Cyber Security Division Director at the Department of Homeland Security.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Power Plant, it was apparently breached.

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

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

(CNN Homeland Security video played.)

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

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

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

So I briefly talk about 10 CFR 73.54 and certainly the licensee's response to the NRC's data request should include how they would address that threat, someone bringing in either a CD, stick or I think they still make the hard disks, although they might be hard to find. The floppy disks I think they call them. So if you bring that type of information into your nuclear power plant, how is that going to be controlled? It would be very difficult I think.

This last slide I'm going to -- next to the last slide, I want to put up here is here's a website. It's called www.backtrack-linux.org. You can pull this up on the web at your leisure. But this is the latest rev. It's called BackTrack 5 R3, August 13, 2012.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And this chart here if you have a SmartMeter and you're an FPL customer you can go to the internet, pull up your account with FPL by typing in your user name and password. And you click on the history usage and all it does is show you how much power you're using at any particular day in any particular hour of the day. And by some magic this utility thinks customers are going to save money because they can see this.

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

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

reasonably achievable.

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

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

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

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

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

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

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

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

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

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

What's relevant on this document, what's really alarming on this document, is this is just one utility. This is going on all over the country. Ninety-eight percent transmission system improvements. And if they have the Smart devices, these devices that are computer controlled remotely, to cause switching functions at their substations so that they can control power back to a service area that is down for one reason or another.

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

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

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

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

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

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

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

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

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

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

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

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

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

And we have a situation here which could bring down the entire electric grid of the United States and affect all 104 United States nuclear power plants. And Al Qaeda has religiously attacked. And so they could take out each grid. They could plan an attack on each grid and take out all three grids at the same time.

And I've personally worked at Palo Verde Nuclear Power Plant and on occasions I wandered out into the desert because I've never been in a desert before. And here I was standing under the transmission lines

and that was the desert.

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

There was nobody within thousands of miles of me. No one even knew I was there. You could almost hear your heartbeat it was so quiet. You could take down the transmission tower. One person could take down an entire grid, that whole section, I showed you on the chart just by taking down that transmission grid. So systems are very vulnerable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. PEDERSON: No, "high assurance."

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

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

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

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

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

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

There is no reason for a nuclear power plant to access the internet in my view. They run fine without internet access. I mean that's the only credible way. If you don't want the computer internet, take the Cat 5 cable out of the computer. Now you're not on the internet. You have to disconnect the nuclear power plant from the internet. That's the only failsafe way to do that in my view.

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

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

I don't know that I saw that on the video. So I wasn't sure what the connection there was between the SmartPhone and the diesel attack.

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

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

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

This came up in one of the videos and again in some of your commentary in presenting the information. Do you have any specific evidence or any other detail related to how or whether or not cell phones can be used to access a nuclear power plant's control systems?

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

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

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

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

CHAIRMAN NIEH: Okay.

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

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

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

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

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

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

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

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

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

hospital to gain access to that material, there you go. So it's a very pervasive problem.

CHAIRMAN NIEH: Okay. Thank you.

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

(No verbal response.)

How about NRC staff that are on the phone? Any questions for Mr. Saporito?

(No verbal response.)

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

(No verbal response.)

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

(No verbal response.)

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

(No verbal response.)

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

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

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

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

CHAIRMAN NIEH: Okay. That will be fine.

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

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

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

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

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

MS. MENSAH: Just ask that.

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

(No verbal response.)

OPERATOR: Yes.

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

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

OPERATOR: I'm unmuting the line now.

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

OPERATOR: Headquarters OPs officer. The line is unmuted.

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

(No verbal response.)

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

(No verbal response.)

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

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