UNITED STATES DEPARTMENT OF ENERGY

ELECTRICITY ADVISORY COMMITTEE MEETING

Arlington, Virginia

Wednesday, June 5, 2013

PARTICIPANTS:

BILLY BALL
Southern Company

LINDA BLAIR
Executive Vice President, ITC Holdings

RICK BOWEN
Alcoa

MERWYN BROWN
California Institute for Energy & Environment

PAUL CENTOLELLA
Vice President, President Analysis Group

JASON CHRISTOPHER
Department of Energy

DR. ROBERT COLES
National Grid

RICHARD COWART
EAC Chair

BOB CURRY
Commissioner Emeritus, NY; Charles River Associates

CLARK GELLINGS
Electric Power Research Institute

DIAN GREUNICH
Dian Greunich Consulting

HONORABLE PATRICIA HOFFMAN
Assistant Secretary for Office of Electricity

PAUL HUDSON
Stratus Energy Group, Austin

SUE KELLY
American Public Power Association

PARTICIPANTS (CONT'D):

CHERYL LA FLEUR
FERC Commissioner

DAVID MARCHESA
Haddington Ventures

RALPH MASIELLO
DNV KEMA

DAVID MEYER
Office of Electricity

RICK MILLER
Consultant HDR Engineering

CLAIR MOELLER
MISO

SAMARA MOORE
White House National Security Staff

GRANGER MORGAN
Carnegie Mellon, Engineering & Public Policy

JAY MORRISON
National Rural Electric Cooperative Association

ERIC OLSEN
Office of Electricity

CHRIS PETERS
EAC Member, Moderator

SONNY POPOWSKY
EAC Vice Chair

WANDA REDER
S&C Electric Company; IEEE

PHYLLIS REHA
Commissioner Emeritus, Phyllis Reha Consulting

PARTICIPANTS (CONT'D):

BRAD ROBERTS
Electricity Storage Association

MATT ROSENBAUM
Office of Electricity

JUDITH SCHWARTZ
To the Point, Consultant Consumer Engagement

TOM SLOAN State Representative, Kansas

MARIANNE SWANSON
NIST

DAVID TILL
Tennessee Valley Authority

GORDON VAN WELIE
ISO New England

REBECCA WAGNER
Nevada Public Utilities Commission

MIKE WEEDALL
Bonneville Energy Administration

JON WORTHINGTON
Department of Energy

* * * * *

P R O C E E D I N G S

MR. POPOWSKY: Okay. Thanks, everyone, for getting here so promptly, we have a full day. Can everybody hear me okay, is this too loud or too much echo? Are you okay? Good. Anyway, my name is Sonny Popowsky, I am the retired Consumer Advocate of Pennsylvania, and I'm also the Vice Chair of this committee, and I'm sitting in today for Rich Cowart, who is our Chair, who is currently addressing an audience in France at the European Commission on some important energy issues. And Rich regrets that he couldn't be here, but he send his regards, I just talked to him this morning, and he thanks everyone for all the work they've done in the last few months to get ready for this meeting.

Why don't we start just by going around the table, because I think there are a few people here who may not be known to everyone, and then we'll hear from David Meyer and then Pat Hoffman. So let's start with the folks at the table and then I'll also ask the folks in the audience to

identify themselves. So, Pat, you want to start?

MS. HOFFMAN: Sure. I'm Pat Hoffman, Assistant Secretary for OE, going into the second round.

MR. WORTHINGTON: Jon Worthington, Department of Energy, I work with Pat as the Deputy Assistant Secretary Office of Electricity for National Electricity Delivery Division.

MR. MEYER: David Meyer with the Office of Electricity.

MR. ROSENBAUM: Matt Rosenbaum, same office.

MR. MILLER: Rick Miller, Consultant with HDR Engineering and participating in the panel tomorrow, I bring an energy storage and a renewable energy integration focus to this.

MR. MOELLER: Clair Moeller from MISO.

MS. BLAIR: Good afternoon, Linda Blair, Executive Vice President at ITC Holdings.

MR. CENTOLELLA: Paul Centolella, Vice President Analysis Group.

MR. VAN WELIE: Gordon Van Welie, ISO

New England.

MS. GRUENEICH: Dian Grueneich, Dian Grueneich Consulting.

MS. REHA: Hi, Phyllis Reha, Commissioner Emeritus, I guess, and now with Phyllis Reha Consulting.

MS. WAGNER: Rebecca Wagner, Nevada Publish Utilities Commission.

MS. SCHWARTZ: Judith Schwartz, To the Point, I am a Consultant in Consumer Engagement.

MR. WEEDALL: Mike Weedall, I'm not quite sure what to refer to myself as --

MR. CURRY: I have a suggestion (laughter).

MR. WEEDALL: Yeah, yeah, yeah. Control yourself, Bob.

MR. MORGAN: I'm Granger Morgan, I'm head of a department at Carnegie Mellon called Engineering and Public Policy.

MR. GELLINGS: I'm Clark Gellings, I'm a Fellow with the Electric Power Research Institute.

MR. MASIELLO: Ralph Masiello, DNV KEMA.

MR. SLOAN: Tom Sloan, State Representative of Kansas.

MR. BROWN: Merwin Brown with the California Institute for Energy and Environment, which is in the University of California, a co director of electric grid research.

MS. REDER: Wanda Reder, S&C Electric Company and IEEE.

MR. ROBERTS: Brad Roberts, Electricity Storage Association.

MR. BALL: Billy Ball, Southern Company.

MR. CURRY: Bob Curry at Emeritus from New York, and I'm now with Charles River Associates.

MR. HUDSON: I'm Paul Hudson with Stratus Energy Group in Austin.

MR. MORRISON: Jay Morrison, National Rural Electric Cooperative Association.

MS. KELLY: Sue Kelly with The American Public Power Association.

MR. TILL: David Till, Tennessee Valley Authority.

MR. MARCHESA: David Marchesa with Haddington Ventures on the corner of David.

MR. BOWEN: Rick Bowen with Alcoa.

SPEAKER: I'm Don (inaudible).

SPEAKER: Good afternoon, (inaudible).

SPEAKER: Elliott Roseman (inaudible) International.

SPEAKER: (Inaudible) Electricity.

MR. OLSEN: Eric Olsen, Office of Electricity.

SPEAKER: Good afternoon, (inaudible).

MS. COLE: Erin Cole (inaudible).

MR. POPOWSKY: Thanks to Jay Morrison for hosting us here this afternoon and tomorrow and our ECA. And I also wanted to thank a couple of our members who will be termed out after this and will be living; Dian Grueneich -- you don't have to leave yet (laughter) -- and Brad Roberts, thank you for your great service for these many years on this committee. And also Ralph Cavanaugh will also be leaving at the end of this session. We are, DoE is in the process of replenishing our

ranks and we hope to have some new members appointed by the new Secretary, hopefully in time for our next meeting in October.

I did want to, just preliminarily, get started, thank the subcommittees, the working groups, your chairs and members for all the work you've done to prepare for this meeting. We have a lot of really good material to go over today, and that's all thanks to the work of the people in this room. I also want to thank the members of the DoE staff who have really worked with this group and worked with the subcommittees, I'd say more than ever before, in sort of a two-way process where they've been able to answer our questions and provide us with input and provide, let us know what they think of our recommendations and vice versa.

So I really want to thank to DoE staff, and I really look forward to their continued participation in our work. We do, obviously, have a new Secretary of Energy, and we're hoping, at least, that we will get a chance to talk to him

sometime in one of our meetings in the near future. I'm sure he's very interested in our work, and I know he's already been talking about some of the issues that we're going to be talking about today. Also thanks to ICF, Samir Elliott, Sherry, and also we would thank Paula Kline for all of her work, she's off to graduate school, I think. Thanks to all of the work that she did for the committee when she was with ICF.

So, with that, let me turn to David Meyer and then to Pat Hoffman.

MR. MEYER: Well, thank you. I don't have a whole lot to add, here. We continue to learn how to make this a fruitful relationship, how to fine tune it and improve it. And I think we've made significant progress in the past year or so, and we will continue. We are in the midst of a transition of sorts at DoE, we, I'm sure we have not yet had all of the meetings with the new Secretary that we're going to need in order to get a clear understanding of what his priorities are and how we can most effectively step up and meet

some of those priorities.

But we will keep you posted and hope to have some arrangement for you with the Secretary for this coming meeting in October.

MS. HOFFMAN: So I also want to express my welcome and thanks, thanks for the members that have been here for a very long time and watching us grow and evolve as an advisory committee, but I also want to welcome the new members and the new faces, some of the folks that haven't been to a whole lot of meetings, and let you know that this is always a lively group, we have very engaging discussions. I want to make sure that what we're focused on is very important and relevant to where the industry is heading and where our programs could head to support the industry, as well as any dialogue or efforts that the Department can do in interacting with other agencies and other activities.

I know you guys are aware that we did do a little bit of reorganizing in our office, and we created a modeling and analysis group which Alice

is temporarily leading right now, acting in this role. And one of the things that we wanted to do was actually strengthen the depth of discussions that the Department is having on various topics, and be able to pull together a group of experts that really could get into the analysis and benefits around some of the strategic thoughts and directions that we're having. And so that's very important to me, I know it is important to the new Secretary, Ernest Moniz, came in, the one thing he said is he wanted us to be stronger in our analysis and how we look at issues.

So I think that's very important. When I had a little bit of time to spend with Dr. Moniz, we talked a little bit of some of my priorities, and I guess I'll just share with you what I shared with him. And then he'll probably, I think he'll continue to, as he understands more of the issues involved in the discussions and the importance of some of the different topics. We did talk a little bit about the synchrophaser activities that the Department has and the

importance of that activity in laying a data platform, or a platform for real time data across the United States, recognizing that's very complementary to some of the modeling that happens in the utility sector, especially at the transmission level, and want to make sure that we develop tools that are actionable by operators, but also get more into maybe some predictive capabilities, modeling capabilities to partnership with the university. So we talked about that a little bit.

We did talk about the importance of cyber security, so the discussion today on cyber security is going to be very important as we continue to mature in this area. We talked about the issues, we recognized some of the strategic directions, and I'll give you some of my thoughts during that conversation, and where I see some priorities are and some of the directions. Energy storage, of course, that was the one thing that he got talons on, and his confirmation hearing was energy storage, so we are diligently working on

the time line and the schedule for energy storage. And I look forward to continuing to work with the subcommittee on energy storage, making sure that we include the relevant topics in the outline for Senator Wyden on energy storage, but have very productive and constructive discussions thus far on it, so we can talk about that a little bit later on.

Some of the other things that I talked to him about was, he actually brought up the natural gas and electricity interdependency issue that was very much, I know, on Burke's radar, as well as on Congress's radar, and I know there were several hearings on the topic. I did go to the MIT Natural Gas Electricity Interdependency meeting, and I know that Allison and some of her team went to several other meetings on the issue, so we're continuing to look at that and try to be more corporate in how we think about that topic and where we need to go. Some of the other things that we talked about that I think are still evolving concepts, at least in my mind, and

probably could use your help.

We talked a little bit of, is there any need to continue to push integration AC/DC, I think IEEE did a magazine article on AC/DC, both at the transmission and at the distribution levels, and one of the things that piqued his interest is DC integrating with buildings, also the use of transactive loads and how do we continue to evolve the electric system with investment in that area. So that was another thing that we discussed. And I'm sure there's other things, I can't remember them all, but I think those were at least the initial topics across the table.

And then, as he is able to come to this meeting as we talk further on some of these issues, I'll continue to give you guys an update on what the Department is thinking, where we're heading, what are some of the major issues. But I think we're still, based on the guidance in the past EAC meetings, I think the discussions and the directions and the things that we're talking about

are very relevant to where the industry is heading. I know that we're still at the Department supporting some of the Hurricane Sandy recovery effort and been asked to continue to look is there an opportunity for utilities to continue to think about microgrids from a utility perspective and how they operate the system. And so we'll work with some of the utilities and different folks in looking at that, looking at that opportunity as a result of Hurricane Sandy.

So that's what I have, at least as my initial update, and I look forward to the discussion, and as I remember more things during the meeting, I'll probably interject them at that time. Thank you.

MR. POPOWSKY: Thanks, Pat. And a couple more folks have joined us. Introduce yourself, Commissioner.

MS. LA FLEUR: Yes. I'm Cheryl La Fleur from FERC, sorry to be a couple minutes late, but I'm here for the rest of the day.

MR. POPOWSKY: And Chris?

MR. PETERS: I'm Chris Peters from Entergy.

MR. POPOWSKY: Okay. Anybody have any questions or suggestions for Pat and the folks at DoE? Dian?

MS. GRUENEICH: We know that Secretary Chu was very committed to energy efficiency, and I know we are going to talk about Race to the Top. Secretary Moniz mentioned energy efficiency, but did the topic come up, do you have a sense whether there will be any diminishment or continuation or any thought, specifically in the world of energy efficiency?

MS. HOFFMAN: Actually, I think continuation there, if I remember correctly, his first event that he did was an energy efficiency event, and expressed his commitment to VEDA, an opportunity that we shouldn't waste in looking at continuing to drive energy efficiency activities. So I don't see a change in that topic at all, from my perspective or my opinion.

MR. POPOWSKY: Okay. Anybody have any

other questions or -- Granger? And, by the way, if you just put your card up, I'll be able to recognize you. Thanks.

MR. MORGAN: So maybe just a comment for the interest of some of you. Clark and I were both just last week at a meeting at the National Academy that brought up 20-some odd very senior folks from China in the electric power area, some of the stuff they're doing is utterly amazing. And the web, the talks will all be on the Academy of Engineering's website shortly, I believe. And so they're worth a look. I mean, just to give you two illustrations, we talk about experimental studies in microgrids, they have 20 of them going on across the country. We talk about moving to higher holdages in DC, they're building many thousands of kilometers of very high voltage DC lines, it's quite --

MR. POPOWSKY: Projects?

MR. MORGAN: Say again?

MR. POPOWSKY: 20 projects?

MR. MORGAN: Yeah. So it's just

incredible.

MR. POPOWSKY: Okay.

MS. HOFFMAN: I was just going to say we're going to make sure that everybody gets the link for the National Academy so they can look at that.

MR. POPOWSKY: Okay. Paul?

MR. CENTOLELLA: This may be too early to tell, Pat, but Secretary Chu came in with an idea about how the Department should structure its research agenda with new kinds of organizational approaches to doing that. Do you have a sense of whether the new Secretary is similarly inclined, wants to take that further, any idea coming from his background about how he sees energy R&D as something that the Department can efficiently organize and pursue?

MS. HOFFMAN: So I think he has a similar approach, but it's probably going to take a little bit of difference with what's on it, and I'm going to say it this way, in looking at the effectiveness of those groups and say how to get

the best things done with the right set of partnerships. I'm not sure that there's a one size fits all, and as the Department continues to evolve, we try different partnership models and ways of doing business. But, ultimately, at the end of the day, we have to take a hard look in saying are we achieving the goals that we hoped to achieve through this partnership.

I perceive him to take a hard look at what we're trying to achieve and the ones that are very effective in the partnerships that are doing to move things forward, I think they're going to be fantastic, and he may tweak some of the other ones that aren't getting us to that results direction that we're going after. I mean, he's very much on the point of how do we demonstrate some successes in the activities that we're working on.

MR. POPOWSKY: Okay. We have a caller from -- (laughter) -- Merwin?

MR. BROWN: Yes. Pat, as I understand it, your conversation with Ernie was focused more

on your explaining to him what your priorities have been and probably will be. Did he give you any indication of what his top three priorities are, issues for the grid research? You mentioned an analysis capability is one of them.

MS. HOFFMAN: I can't say that he gave me, you know, these are absolutely my three top priorities. I mean, the thing that he recognizes is investment in the grid is paramount. I mean, he said that several times that he recognized the importance of investing in our infrastructure as a support network for the economy, but we need to continue to evolve and grow our infrastructure. He recognizes the complexity. So the other thing that he brought up is he understands this is a very, very complex, difficult issue, area, and really no silver bullet, you can't find a silver bullet, you're going to have to work through some very tough issues, and that there are regional differences across the United States, different market structures, different things that we have to keep, pay attention to.

So he recognizes the complexity. So, from my perspective, I got the sense he really feels the electricity area is an important area, and he wants to continue to support the research and the discussions in this area, but recognizing that it's complex and there's no silver bullet.

MR. CURRY: When you mentioned the various things that you were focused on, one of them was working with utilities on -- did I get it right -- distributive generation? And how does that, would these be utilities like our favorite in New York, the Long Island Power Authority, which is a public authority. Otherwise, how do you get access to utilities under the current framework of the Sandy legislation?

MS. HOFFMAN: So, some of the activities that are done are allowed under the CDBG fund, and some of them are allowed under existing FEMA funds, but those are limited in scope. So the other areas that we can do is just provide technical assistance with the labs to help analyze what one would look at if, you know, in

partnership with the utilities on microgrids and how they would look at the opportunities there. Granted, that utility structure is different, so it's more from our perspective that we're looking for a couple, to work with a couple communities on some pilots that would help with the analysis.

We wouldn't do the infrastructure investment or anything along those lines, because that would go through the traditional mechanism, but what we're hoping to do is help people ask the right questions and analyze the issues and say, if you go down this path, here are some things that you need to think about. And what we're looking at is taking some of the lessons learned what we did with the OG in looking at how do you optimize. I mean, I'd like to say it's more of an optimization discussion, but also resiliency discussion.

Internal to the Department, we had, I'd say, a fairly long discussion on what does it mean to be resilient, and I think everybody has a different definition for resiliency and their

expectations, and so one of the things that we wanted to do was help facilitate that discussion on what does resiliency mean, how does that translate to infrastructure, and thus how does that translate to customer expectations, restoration expectations. So those are the type of things that we're trying to just aid and facilitate the discussions on, we're not looking at the hardware investment, because there's traditional mechanisms and limitations.

Limitations under the Stafford Act, I think the states are probably going to consider what they can do from the codes and standards point of view, and if you can change some of the codes and standards, then you can affect the infrastructure investment from a hardening point of view. I mean, I look at what Florida has done and the southeast has done, and how they've, slowly, over the years, changed some of their codes and standards and some of their practices. I mean, it took some time, but they evolved to harden their system. And, once again, this is not

going to be an overnight transformation, but I think there's ways that we can start thinking about what some of those best practices were, especially what was done in the southeast and say what can the northeast pick up from that.

MR. CURRY: Just an observation of, Con Ed has a rate case pending in New York state now, asking for roughly a billion dollars over the next four years for storm hardening. And the city of New York filed 400 pages of comments on Friday taking issue with almost every single point that Con Ed put in their rate case, so if anyone on your staff is interested in an entertaining trip through, this is what we really mean, it's available. And I can also connect them with the city people who put the 400 pages in, and they were very proud of those 400 pages.

MR. BROWN: Thank you. Since we've gotten to this topic about resiliency, it's been, obviously, a hot topic with regard to storms that blow a lot and rain a lot. But I would hope that, in that conversation, unstated, his concerns about

wildfires and earthquakes and things like that, which is a bigger problem in the west.

MS. HOFFMAN: I don't disagree with that, and by all means, we're looking at all hazards. But I think it goes back to the regional risk equation of what are the risks most likely for different regions of the country, how they want to define their resiliency, what do they want to build towards, how do we start a procedure for or a process for engaging in that conversation so that we're not kind of thinking about it after the event occurs, but trying to get really more proactive in looking at resiliency for the United States.

But I still go back to, I'm not sure everybody's on the same page, what resiliency means and what do they want to build towards, and a matrix or a definition for resiliency.

MR. POPOWSKY: Okay, great. Thanks, Pat, I assume you'll be here for the next two days?

MS. HOFFMAN: I'll be here.

MR. POPOWSKY: If anything else comes up that you want to hear from Pat on, I'm sure she'll be glad to chip in. I just want to say, Commissioner La Fleur, it's up to you, if you would like to go next, we could shift the program, or -- depends on what your schedule is.

MS. LA FLEUR: Well, I'm here for the afternoon, so I'll do whatever you want. I'll go next, or you can go next, or --

MS. HOFFMAN: Go ahead.

MS. LA FLEUR: Okay, all right. Well, thank you very much for having me, Sonny, and Elliott had asked me to do an update on some of the goings on at FERC where it's been very, very quiet and not newsworthy for the last couple of weeks. First, I want to introduce somebody I have with me who is a summer intern who started in my office at FERC just this week, I'll ask him to stand, Daniel Jang.

Daniel is a sophomore at Princeton and comes to us underwritten by the Princeton -- whatever it is -- Princeton in Civic Service

Intern Program, and he's in Operations Research and has done work, among other things, with the Princeton Co-Gen and their own microgrid. Not as many as China, but they do have one that stayed up during Sandy. And so we're really, I didn't plan to hire a freshman when we went out to interview, but he was the smartest kid we saw, so he'll probably be running FERC by the summer.

(Laughter)

Okay. What I thought I'd do today is, I was asked to talk about Order 1000 compliance, which is actually the first time I've tried to weave together what we've put out so far into a summary, so we'll see how I do. Talk a little bit about cyber security, which I know we have later on in the agenda, and just some other newsworthy things that we've either recently voted out or have coming up that you might want to have on your radar screens. I always say this, but it seems particularly important right now, with all the dissent and all flying around on some of our orders, I only speak for myself, not for the

Commission, and I will try very hard not to comment on pending open dockets, to be a historian of what we voted out, not a predictor of all the rehearings, appeals, and compliance dockets and so forth, on into the future.

So, so far, we have voted out, I should know, maybe six compliance orders under Order 1000, we have at least four big ones still ahead of us. And we've tried, as I think you can probably see, each month to do ones from different regions of the country to kind of equalize the staff work, and we've tried to be taking on both the regional transition organizations and ISOs and the bilateral market regions of the country so we can be voting those out in tandem. Just sort of try to summarize a few of the trends that we're seeing so far, dividing it into the big elements of the Order in the first place, starting with transmission planning, Order 1000 at basis required that each public utility transmission planner had to participate in a regional transmission planning process that satisfied the

principles of Order 8-9 in the transparency, fairness, and so forth, and produced a regional transmission plan.

And so every single order starts with a sometimes perhaps laborious review of the transmission planning process submitted. And, for the most part, the orders have largely confirmed the regional processes already in place in the organized market areas of the country. In many cases, we've pushed back asking for more detail on certain elements of the process and how they were going to select the projects that were best for the region for regional cost allocation. In the bilateral regions of the country, we've pushed back somewhat more on asking the regional planners, which we recognize are sometimes just a few jurisdictional utilities with a lot of non jurisdictional in between them, to come back with how they, as a planning body, are going to select their projects rather than, I call them the staple plan, just kind of putting to the everything everyone was doing already and calling it a

regional plan.

And so, really, in all cases, we've had compliance requirements imposed that they have 120 days to meet. The biggest thing changing in planning was the public policy requirement, Order 1000 required that both local and regional transition planning processes, in addition to looking at reliability projects and economic projects, had to consider transmission needs driven by public policy requirements that are established by federal and state laws and regulations and have procedures to identify the transmission needs driven by public policy requirements and evaluate proposed solutions. And this is where most of the action has been, particularly in the RTO regions on planning, since they already had planning processes.

Most of the compliance requirements that are still out there have been tied to the issue of the role of the states in determining what are the -- I think Order 1000 clearly suggested that the states would come forth with a compendium of what

the public policy requirements are, because they're in large measure drawn from state law and regulation. But we have said thus far most of the compliance orders that is the planning region, the ISO, or the planning body that had the responsibility to come up with a proposal to select the projects that meet those public policy requirements, rather than delegating the selection to the states.

There's been some nuances, PJM had a proposal, has a proposal for a state compact where states could get together and voluntarily sign up. ISO New England had one that was somewhat quite similar. In the PJM case, we said you already have public policy requirements based into your planning some other place, so that meets Order 1000, so the state compact can go forward as a complimentary element, even though it, because it didn't meet Order 1000 all by itself, but because you have this other thing, and I think we said something somewhat similar in ISO New England that we were not in any way prohibiting the state

proposal, but that there had to also be a complimentary effort at the regional level. And so those are still pending.

Big action as anticipated, and most of the dissents, and public commentary on this have come along around the element of Order 1000 on the rights of first refusal. Basically, Order 1000 requires that public utility transmission providers had to remove from commission jurisdictional tariffs and agreements, a federal right of first refusal and exclusive right to build transmission facilities in a particular incumbent's footprint for projects that were going to have regional cost allocation, subject to certain limitations that incumbents could still build what they needed to for reliability and pay for it themselves, that we wouldn't affect state laws that gave people exclusive rights, wouldn't affect rights of way and property rights, and there's a back shop that something is being done regionally and it's not coming on in time to meet a local need, and I forget if there's a fourth

requirement, I just lost it, but there are some exceptions already in the rule.

This is what most of the thorny compliance issues have come around. The first threshold issue we deferred until compliance some legal questions about what were the standards of review that would govern the Commission's look at the rights of first refusal proposals, and there was a suggestion that the Transmission Owners Agreements in ISO New England, PJM, MISO and SPP. And SPP is still pending, but the other three I can discuss were voted out. The question of whether the Transmission Owners Agreements were themselves contracts entitled to Mobile-Sierra protection, so they could only be amended if it was a violation of the public interest. And we decided in the first round of cases in PJM and MISO, I think were the first two we voted out, that they did not get an automatic public interest protection because they weren't developed in the kind of arm's length commercial; I'm selling power to you, what are you going to pay for it, what are

the terms, because they were developed by people with common interest with respect to the right of first refusal.

So having reached that conclusion, in the New England case, there was a follow-on legal issue that there is a 2004 FERC order approving the New England Transmission Owners Agreement that specifically approved some terms that gave public interest protection to certain components of the Transmission Owners Agreement. And we recognized in the order that that meant that those elements of the Transmission Owners Agreement could only be changed if there was an actual public interest need rather than just because they were no longer deemed to be just and reasonable. And we spent a considerable amount of -- I spent, actually, a considerable amount of time reading all the Mobile-Sierra cases back to Order 888 and Order 636, a little walk down memory lane.

Actually, considerably off memory lane, since I didn't remember most of it, of what did it mean to have a public interest standard and how

would we parse that, and trying to really figure out was there a space where something could be not just unreasonable, but we could say to the people in new England or someone else, don't worry, you can pay non just and reasonable rates because it's not against the public interest, and what is that space in this area. And I think what ended up coming out was the recognition that the taking away the rights of, we ultimately ruled that there was a public interest requirement to remove the rights of first refusal, because the introduction of transmission competition was important to make sure that the rates were fair and the right things were built.

And that ended up, I think, being an acknowledgment of the significance of what we were doing. I mean, I've actually been making speeches for a couple of years comparing this to generation competition, but I think there's been a -- a lot of it was writ out more clearly in some of the orders we just put out than had been before. Probably all I can say about that. There were

also some issues about -- some considerable issues about what kind of reference could be made to state's statutes and federal tariffs, and so far, I guess summarize the orders we've put out to say, the state's statutes are what they are, as far as -- I've never indicated that they were preempted in any way, or that's never been said in the order, but they can't be codified in the federal tariff, because they would give them a new federal right of first refusal, and we can talk about that offline, but that's another, that's a very detailed part of the order.

Finally, the last part, cost allocation, we asked all the transmission planning regions to come forward with a cost allocation proposal that had to satisfy a bunch of principles, of which the most important was that cost had to follow benefit. We said we would accord regional flexibility, and I think we have, particularly in this area, given, shown quite a bit of regional flexibility. PJM, I think, was of the RTO's made the most change, or one of the ones that made the

most change in their cost allocation proposal, came forward with a hybrid approach for projects over 500 KV, we approved that. MISO made some changes in the definition between local and regional, and what they would cost allocate, that was approved. There's some others still pending and some that have been pushed back for more detail on certain things, and, as I said, we have four more of these coming.

In terms of next steps, we voted out 120 -- in all cases, the next step is coming up in 120 days, so that's imminent, that is 120 days, and Clair probably knows from the first ones. Right around the corner in July, the interregional compliance filings are due, some are already in, I haven't really looked at them well enough to make a speech about what they say, but we will be digging into those, obviously. And, not to be forgotten, I guess it's not surprising, given what's afoot, here, that there have been considerable legal challenges already to Order 1000, and I am sure there will be more, as the

compliance issues get worked through.

So those have been assigned to the circuit court in the District of Columbia. There was some question of which circuit it was going to go to. And the court has worked out, I don't have it at the top of my head, but a very detailed briefing schedule on issue by issue that I think will go into the summer and fall, so we'll be working through the legal side while we're simultaneously working through compliance side.

Do you want me to keep going? That's all I was going to say on Order 1000. I think -- all right. So that's it on Order 1000, I'm sure I've answered all your questions, all is clear (laughter). Just turning to cyber security, a little bit more. While the Hill continues to debate various legislative proposals, at least within the electric system of the electric grid, FERC does have the responsibility on the Section 215 reliability standards require that we approve standards to prevent cyber security incidents, and I have said it's kind of like the iPhone, with

iPhone1 and iPhone2, and you go buy a new one, they tell you a new one's coming, don't buy that one.

Well, we're on iPhone 5. Five was approved in May, and -- I've said this is just like, my daughter broke her phone, and they said don't buy a new one because six is coming, like, in two weeks, just cobble together the old one. The industry came and said we don't even want to bother with SIP 4, let's just go right from SIP 3 to SIP 5, because it costs so much money every time you do something new. And we approved that, we largely approved SIP 5, asked some questions about the implementation schedule and a few other things.

Basically, in a nutshell, SIP 1 through 4 were about designating what was a critical cyber asset, who designates what the critical cyber asset, how critical. Now SIP 5 is a different approach, it says everything gets some level of cyber protection, but just the most important things get the most and the things that impose the

least vulnerability in the system gets the least, which was one of the things we asked is what they do get, a nerve to come back on. So it still will not get us out of the characterization, but it reduces the all-or-nothing characterization.

In the meantime, President Obama, as you all know, put out an Executive Order, I believe it was in February, on cyber security, calling for more information sharing, as well as the development of a voluntary cyber framework. FERC, because it's an independent agency, isn't actually covered, whatever that means, but we've announced that we're voluntarily doing it. I think I've talked about it in this room before, that FERC has set up an Office of Energy Information Security, and Joe McCohen's group has been meeting with folks in past groups, the states, NARUC, Department of Homeland Security, and really anyone that wants to meet with us to try to do things together, and I think that process is subject to anyone else's thinking of developing that voluntary framework is making progress.

Other reliability orders, in May, we -- I've been, I talked about geomagnetic disturbances at this table before. In May, we voted out a final rule on geomagnetic disturbances, I'm sure people might disagree, but I think we were somewhat quite responsive to some of the comments we got, not just in changing the timeline, but also in getting more flexibility in compliance. It basically requires the development of a standard on procedural response, what you would do if there were a massive solar storm in terms of operating procedures, kind of like a storm plan that you have for hurricanes or tornadoes. Six months for that standard, 18 months for a bigger standard.

That would include an assessment of vulnerability and a plan which would vary by equipment, location, geography and so forth, or how to mitigate those vulnerabilities. This is something where, as a standard gets developed, we're also learning more about what we're protecting against, but it's going to be such a

long-term, multi-phase effort, I've been a big advocate of we should get started, and I think this is an important step.

A couple others, just wrapping up, July 9th, we're having a technical conference on reliability, because who wouldn't want to come to Washington in mid July for a reliability conference? We previously, I think, have done this in, like, the early part of the year, and Jerry Cully and the folks at NARUC asked if we could do it after their annual reliability report came out, which seemed to make, actually, quite a lot of sense, so we're doing it after the report came out in May.

And, so, we'll look at the annual state of reliability, probably -- the agenda is not out yet, but certainly priority, what NARUC is working on, and I think we'll ask NARUC to talk about some of their major efforts on the reliability assurance initiative, which is their compliance restructuring, and the standards, and maybe some other things. Gas Electric, we had the last tech

conference in April, we are working on next steps on the communications, Gas Electric communications, whether we need to clarify anything there. So watch this space for something on communications, following up on the tech conference in February. In the meantime, I see Gordon and Clair and others are working within the regions on proposals for this winter and beyond, and we're closely following those efforts, but I think communication is, in terms of something to expect from us, the next thing we'll think about.

And, finally, some of you might know, I've been clamoring -- well, maybe clamoring is a strong -- gently agitating for a technical conference on capacity markets, and it looks like we're getting some traction, so we hope to have one in the fall at some point, to be announced. Really looking, and I guess my reason for calling for this is, since I've been on the Commission, we've probably done 30 or 40 cases on capacity markets, and many of them are extremely specific. New York City taxes and cone, fuel cells and PJMs,

zones. Very, very narrow. And the things, the big picture of, like, how far out in time should you look, what should be covered, how should exemptions work, we can never talk about because it's always ex parte because we always have cases pending.

So the idea was to kind of take a step back and take a look at some of the big philosophical issues, are they working, how they're supposed to work, which things different people do it differently, how is it working, what might change in the future with things like gas, electric coming down the pike, and the state renewable requirements and how they fit in, different places with demand curve and not with demand curve, and so forth. So it's a tall order to even put together an agenda, but there's plenty to talk about, and I think the concept is, at a minimum, maybe we'd learn something that would inform us as we went back to looking at the narrow cases, or inform the stakeholder processes, dare we hope people learn from each other, it's a dream

that we can all share.

Or -- and I'm being sarcastic -- I know people do learn from each other, but these are all so well developed in different structures, it's hard sometimes to even talk about them together. Or perhaps there will be something affirmatively that comes out in Commission policy, but that's by no means preordained. It just seems there's plenty of talk about, so that will be something to, we'll be looking for, I'm sure, broad participation from folks who run capacity markets, are thinking of it, don't run it and you do just fine, et cetera.

So that was what I wanted to say, Sonny, or maybe not what I wanted to say, what you wanted me to say, hopefully, and I'll be happy to take questions.

MR. POPOWSKY: Okay, thanks. Before I ask questions, let me make sure that we all thank Commissioner La Fleur, who is our official liaison, FERC liaison to this committee --

MS. LA FLEUR: I actually added it to my

bio, so that's about as official as you get (laughter).

MR. POPOWSKY: And has really done (applause), we really owe her a great -- thank you for taking the time at each of these meetings, and reporting to us, hearing from us. So thank you very much, Commissioner La Fleur.

MS. LA FLEUR: Printing from what you're all doing on storage and transmission, and some of the things you work on.

MR. POPOWSKY: Great, thanks. I'm sorry, Pat, did you want to go first before we --

MS. HOFFMAN: I can take my turn, like everybody else. Just a couple comments. One thing I forgot to bring up that, Commissioner, you should keep in mind is, I know that Dr. Moniz is doing a quadrennial energy review, and that something that even the states should think about, because I know the states are doing their energy plans, and how we can see if we can pull some of those threads together in looking at the energy strategy, the infrastructure requirements. So

just something to keep in mind.

I know it's a little bit one-off from some of the things you're working with, but I think it's something that we could, hopefully, if done right, could probably bring some parallel pieces together. The second thing is, I know I was in a meeting with some of the industry folks, Chairman Molenhof and Joe, and I know that Joe McClellan's doing his own kind of maturity model Q&A questionnaire for utilities, and there was a strong ask that the federal government get together and -- how should I say -- gain some consensus from different assessment pools that are out there, because we have our maturity model and Joe's developing a questionnaire type format, and there was a request to make sure that we try to pull that stuff together. So I just wanted to put that on your radar.

MS. LA FLEUR: Well, first of all, on the quadrennial energy review, whether we have any direct role, which we'd probably welcome, but it's definitely, what comes out of that then indirectly

informs things that people then subsequently file with us, so I'm very happy it's happening. I've heard somewhat similar things on the different tracks in government, so maybe we can take it offline. It certainly makes sense to work together.

MR. MILLER: Thank you. Again, Rick Miller with HDR Engineering. I offer this comment and question with a little bit of trepidation, my first time here at EAC. My background is over 35 years in grid operations, energy storage, and I'm past president of national hydropower association. We, as an association in the hydropower industry have done a bit of work with FERC, with Arnie Quinn, Mason Emmitt, and the team on markets and recognizing strategic flexibility.

What, from a Commissioner's perspective, what guidance or insights could you provide to us or to the industry with regards to how do we help create linkage of the Office of Electricity and DoE and FERC to help present the most, what's happening out there in the grid and create that

linkage? Maybe some consensus from that, back again to the federal government to more of a stronger voice. Some insights from you, Commissioner, would be helpful.

MS. LA FLEUR: Well, thank you, Rick. I'm not sure I have a lot of insights about how you help us work better together, but it seems like groups like this, other things that we do with Pat's office and Bill Brian, and people like that are important to understand what we're each doing. In terms of hydro, I had made a comment when I spoke at the National Hydro Association, I think, in 2012, that I think it's important that we hear from the hydro industry. Most of the hydro work that we see at the Commissioner level is very micro, appeal from some license suspension or, you know, it doesn't get that policy-ish.

I mean, it's policy of how you move the hydro licensing around and what gets an exemption and all, but in terms of increasing the profile of hydro in shaping the markets, that's not going to happen in the individual hydro dockets. And I

think I've made the comment that hydro can be a little bit of a taken for granted resource, because with some unique exceptions up in Alaska and so forth, we're not seeing a lot of big hydro development anymore, it's more small hydro development and increasing output along the edges. But I think the hydro folks need to get in the conversation on what they can help do in the places where you can still run your hydro this way, to help balance other renewables, and as kind of a storage resource.

Storage is very sexy, hydro is not sexy, but hydro is storage, in a way. So I think it's communicating what you can do in the same way that the flywheel people and the battery people, I think, have been effective in getting their voices heard on frequency regulation, teaching us what we didn't know. Hydro, I think, maybe could have a bigger role there.

MR. MILLER: Follow up. Is that most effective through dealing with FERC and Office of Markets, or the Commission staff or through the

Office of Electricity? Give us some insights there.

MS. LA FLEUR: In the Office of Electricity at DoE?

MR. MILLER: Yes.

MS. LA FLEUR: Well, I can't -- I mean, that sounds to me to be a good thing to deal with them, also. In terms of FERC, I think, I usually tell people to really know the staff that regulates you, so, in your case, it's probably most likely Projects. On some of these more forward-looking things, the Office of Energy Policy Innovation, and if it's, when you have the time and opportunity to go to the five Commissioner's offices -- I know that the Stations of the Cross can be slow, but it's good for us to hear it. But never skip staff, always go to staff and the five Commissioner's offices.

MS. GRUENEICH: One question and then one comment on the upcoming fall conference. Is there any place where FERC hosts like an annual meeting of all of the ISOs and the RTOs? At the

last NARUC Sunday collaborative, there was an informal presentation by each of the ISOs and RTOs that I felt was tremendously useful just because, in one room, you heard different aspects. And, to me, it was so interesting to understand the governance of each of them is quite different. So that was my question. Is there any hosting like that done by FERC?

MS. LA FLEUR: To the best of any knowledge, it's not something we've done, like, on a regular basis. And perhaps we should. And I was at that NARUC meeting and would agree, it was excellent. In, I think, early 2012, but maybe it was early 2011, because my years are running together, we had all of the RTO/ISO presidents come in and talk about the matrix report at a regular open meeting, which was actually one of our best open meetings, I think. Maybe that's damning with faint praise, some of them are very short, but that was really meaty, and I thought, very good.

Now, recently, we've established much

more targeted having all of the RTOs come in and talk twice a year about what they're doing on gas/electric, and we did that most recently just in May in a special session. But it wasn't all the CEOs necessarily, as the first one was. It's something to think about. I don't want to make a trend where a trend doesn't exist, but the last couple of open meetings, we've tried to put things, the chairman had tried to put things on the docket like the gas/electric, and then we have the capacity portability kind of a report at open meetings.

There's certainly scope to use that forum more than we do, because we do get a little bit of tech conference overload, where you can only have so many tech conferences.

MS. GRUENEICH: And I wasn't suggesting it, I just think it's interesting to think about maybe on a periodic basis. So my comment, then, is, I think that the upcoming technical conference on capacity markets is going to be excellent. As I'm sure you know, in California, there is a huge

debate going on, and to the extent that there's any sort of a briefing book that would be made available beforehand electronically that, again, would be sort of here's approaches of the different ISOs and RTOs, here's our experience, I think that would be extremely helpful, since, obviously, not everyone's going to get to D.C., or wherever it is.

And I would just put in a plug for some of the issues, at least, of concern, I think, are what is really the relationship between state public policies and the capacity markets. I've heard both ways that there are ways that it can be written into tariffs such that there's sort of a federalization of a state policy, I've heard the opposite that it can't be done. Another area, I think, of great interest is on the demand response. And not just what do we know about it, is it just least cost demand response, is it able to be coming in over different times.

And then my third area is energy efficiency. In the research that I've done, I've

not seen capacity markets really pick it up, it pretty much seems to be demand response, and especially where states are looking at comprehensive, more complex types of approaches on energy efficiency, is the capacity market another tool, how does it work out? So I think those would be useful.

MS. LA FLEUR: Well, those are great suggestions. I agree with you on some kind of a staff briefing book or something would be really helpful, and I also agree you've raised really interesting issues. I think, on energy efficiency, the PJM press releases that came out within the last couple weeks on the most recent, their most recent RPM option saw an increase of energy efficiency in that market, and you're talking next to the, sitting next to the right man for how they model it in New England. I should also say, in addition, I'm talking about a kind of a think-y piece capacity market conference.

We did say in an order that we were going to have a joint tech conference with the

CPUC on -- and I think, I honestly don't know if it's been publicly announced, but it's sooner than the other one.

MS. GRUENEICH: I think --

MS. LA FLEUR: Yeah, I think it's June 31st, I think it's the end of July, July 29th or 30th, or something like that. But that one's already announced, I think, yeah. I'll be around, so we can talk offline, if people have questions, or I can ask you questions. Thank you.

MR. POPOWSKY: Thanks, again, Commissioner. I'm going call on myself next to lead the discussion of Race to the Top. So I'm going to go there, if you could pull the slide up. Thanks. One of the tasks that Rich asked me to do before he left for Europe was to head up this working group on the Race to the Top initiative. This is a working group, as opposed to a full blown standing subcommittee.

So we're here to the a couple of tasks, and we may or may not continue after today, but in any case, one of the things we wanted to do was to

get some recommendations to the Secretary, to DoE in a timely manner so that they would be useful in the upcoming consideration of the Race to the Top proposal, which hopefully many of you are familiar with. But just to start out, the working group, I'm the chair, Bob Curry is the Vice Chair, we have a good cross section of members from this group on the working group; Ralph Cavanaugh, Sue Kelly, Paul Centolella, Dian Grueneich, Val Jensen, Paul Hudson, Phyllis Reha, Ralph Masiello and Mike Weedall.

Janine Migden-Ostrander from Wrap Staff has been assisting us, and also Holmes Hummell from DoE, who has really been the leader, I'd say, on the DoE side of the DoE staff, and really developing this whole idea and this project, has been able to attend most of our meetings and has really been extremely helpful in all of our discussions.

Just to go back, actually, most of you remember, we actually had a couple of telephone conversations on this issue, informally, among

this group, not acting as the Energy -- as the Electricity Advisory Committee, but just among the members, some initial conversations that Rich set up to talk to DoE staff about the concept of Race to the Top, even before it was publicly announced. And I think that those conversations were helpful, each of us as individuals had a chance to make some comments to the DoE staff in developing this proposal, and I think a lot of us were very pleased to see that, lo and behold, the President's State of the Union address came out, this issue was included.

Now, the actual language that the President used in the State of the Union on February 12th, he talked about a new goal for America, cutting in half the energy wasted by our homes and businesses other the next 20 years, and said we'll work with the states to do it. Those states with the best ideas to create jobs and lower energy bills by constructing more efficient buildings will receive federal support to make that happen. Now, he didn't use the term Race to

the Top, but if you look at the State of the Union blueprint, which was a written document that came out simultaneously, the same day as the State of the Union, there was a little bit more meat put on the bones of the President's proposal.

And, in that blueprint, they specifically talk about an effort to double American energy productivity by 2030, starting with a new, an energy efficiency race to the top for the states. The idea was that, using as a model the Race to the Top in the Department of Education to try to give states the incentives, the ability and rewards for stepping forward, particularly in the area of energy efficiency and productivity, and reducing waste. And there's a point there, the last sentence, which I think is important that, while the focus is on energy efficiency and productivity, it was recognized right from the start that not only will these programs save consumers money, but that resulting reforms will drive investments that enhance manufacturing competitiveness, improve grid

resiliency, and cut carbon pollution.

The DoE budget proposal came out in April, the President's budget included a program for fiscal year 2014, it was actually a two-step or a two-phase program. Phase one is a qualifying phase, that is qualifying criteria are established, will be established by DoE that would include policies that states -- and, by the way, when I use the word states, and we'll get to this a little bit more, but we're referring also to public power, co-ops, tribal utilities. But the idea was that states and these entities would implement policies to encourage cost effective investments in efficiency, including combined heat and power and demand response, clean distributive generation, enhance customer access to data, investments to improve reliability, security and resiliency, and enhance sharing of information regarding grid conditions.

Those are the general criteria that would go into the qualifying phase of the Race to the Top. Then phase two, those entities, those

applicants that qualified, that met the DoE's qualifying criteria would then have the opportunity to compete for cash awards based on, and I quote here, "The most progress toward improving energy efficiency and energy productivity." The proposal is for a $200 million appropriation that would be in fiscal year 2014, but I believe the money could be spent anytime between 2014 through 2018, as proposed by DoE. $15 million would be used by DoE to oversee the program, $25 million for phase one would be put to provide technical assistance to assist the applicants in meeting the qualifying criteria, and then $160 million for phase two awards.

We had a number of meetings, we met on a biweekly basis, the working group, recognizing that our primary job here was to get something to DoE reflecting the views of this committee regarding the Race to the Top proposal, in a way that would be useful to DoE in these upcoming discussions over the next several months. And our overriding conclusion, I think, certainly the

unanimous conclusion of the working group, is found here, which is that the DoE, at least from the working group perspective, we have reviewed the Race to the Top proposal and fully support this important initiative.

What we recognize is that many of the most critical, and what I think the President recognized, actually, was that many of the most critical factors, policies that can support energy efficiency and energy productivity do occur at the state level and at the utility level, and that by supporting this Race to the Top concept, there's really two benefits: First, it rewards those states that make the most progress in meeting the energy goals established by the President and by DoE, considering their individual circumstances; and second, it identifies successful models that other states can follow in the future in their own efforts to achieve these goals.

We did have some very lengthy active discussions among the members about some of the specific recommendations that we wanted to make to

DoE in pursuing this initiative, and I'll just go through them with you. There are five, and, by the way, hopefully, all of you have with you the draft document that we are proposing to send to DoE, if it's approved by the committee today. It looks a little bit like this, it's essentially a letter from Rich Cowart to Pat Hoffman, setting forth the EAC's views on the Race to the Top proposal. So these principles, like I said, we came up with five principles that I think we had universal support for among the working group members, but not everybody got to attend every meeting, so, certainly, we can hear from folks today whether you were on the working group or not.

The first principle is that the Race to the Top should allow participation by states and other eligible applicants with all types of utility ownership and business models. The point being here that we know that not all of us are served by, or work with or work for investor-owned or state-regulated utilities. We also have,

obviously, public power, co-ops, tribal utilities, all of whom we think, or at least the working group thinks should be eligible to participate in this program, to fully participate. Even in the investor-owned utility arena, we have different types of utilities. We have some states that are with vertically integrated utilities, some with restructured utilities where only a portion of their service is actually regulated by the state regulatory authorities. So, as we develop this Race to the Top, we wanted it to be all inclusive, to include all types of utility ownership and business models.

The next principle is in phase one. The qualifying criteria should be descriptive rather than prescriptive. That is, allowing the states and other applicants flexibility to innovate. And when we, once DoE determines what the overall general criteria should be, that should be done, in our view, in a descriptive manner rather than prescribing specific, very specific programs or policies that absolutely have to be met by each

applicant, as long as those policies are designed to achieve the overall goal of energy efficiency and productivity.

The next principle, which is the third one on this slide, is that, in phase two, remember, that's the reward phase, the ultimate phase. Race to the Top applicants should be judged and rewarded based on their own improved performance. This arises from the concern that we know that all these states, or many of these states and many of these other applicants are starting from a different place. You have to think of this, it's hard to not use supports analogies when you think of this process, but we know that some states are starting off on the opponent's ten yard line, they don't have that far to go. We know that other states are probably on their own, practically on their own goal line, that's where they're starting from.

And we want to make sure that those states that get from their own goal line to maybe mid field or maybe to the opposing 40 yard line

gets, has the ability to get some of these rewards, rather than limit the ward to those states or those entities that finish across some magical finish line first. Because the concern is that, if there is just this one finish line, we sort of know from the start, or we have a good idea from the start which entities might win, whereas what we really want to do is, at least in our view, from the working group's view, is to reward those states and applicants who make the most progress in achieving these goals. So it's based on their own improved performance.

Having said that, remember, though, these states have to have met the initial qualifications established by DoE to participate in the programs. So there are some minimum qualifications, but within that group of applicants, we want folks to be judged on their own performance rather than the first across a finish line. The last two recommendations, basically, we support the two-phase program; phase one funds should be used to support the

development of innovations, programs, policies, regulations and/or laws that advance energy efficiency and energy productivity. Whereas phase two awards should be made based on the achievement of improvements in energy efficiency and energy productivity.

The first phase is basically designed to encourage the development of policies that will get us to, that will help the states get to where we all hope that they will go, the second phase, the rewards are based on performance, actually implementing some of these proposal and who make the most, who achieve the most improvements in terms of energy efficiency and energy productivity. The final principle is just that the RTT awards should be focused on achieving improvements in energy efficiency and productivity.

What we're saying there is that those are the goals; energy efficiency and productivity. Now, I think, at least I believe that energy productivity is a broader concept than energy

efficiency. Typically, I think energy efficiency, what we're talking, I think most folks are talking about end-use efficiency. Whereas energy productivity is a broader term, it includes basically any way to get your economic output to be provided with the fewest or the smallest possible energy input. I think that's right, Paul, what do you say?

Anyway, and that can involve any number of programs that go beyond the classic or traditional end-use energy efficiency. So we want to focus on a broad view of energy efficiency and productivity, but that is the goal; greater energy efficiency and productivity. And, as was pointed out in one of the earlier slides, the State of the Union blueprint points out that those factors, that those policies that improve energy efficiency and productivity have also benefit the grid in terms of greater reliability and greater resiliency, they provide benefits in terms of reduced carbon pollution and other factors.

So, hopefully, you've all had a chance

to take a look at this. Let me call on Bob and Holmes first to see if you have anything to add. As I said, Holmes Hummell from the DoE staff was instrumental, maybe the prime architect of this idea, and whatever, if you'd like to add something, you and Bob, and we could hear from other members of the working group, and then all the members of the committee.

MR. HUMMELL: Good afternoon, everyone. I want to thank the subcommittee for giving attention to the concept, I cannot claim to be its architect, so it would seem flattering for all the attention the proposal has received. In fact, the Race to the Top is borrowed directly from the success the administration had achieved in other parts of the policy portfolio, including health and human services and education. We understand the distinct differences between energy and those other parts of the portfolio.

What you're seeing in this proposal is an approach that is innovative in terms of federal relationships with states, that reserves to the

states the full flexibility of achieving objectives that still serve national interests and the goals of many state leaders. The material that's in the public domain about the proposal is fairly limited, only three pages, so I think it's impressive that the subcommittee members have cultivated their views on the concept, with real deliberate thought to the detail and its potential, while knowing that there's still very much about the program that's yet to be designed.

The Department is operating under a continuing resolution that actually says in black and white text that we are forbidden from even issuing a request for information to invite stakeholder input on this proposal until it is appropriate rated. For that reason, members of the FACA here, and the FACA that serves the State Energy Advisory Board members are the two places that we can go to seek policy input in a public setting that would allow us to continue to cultivate and develop the idea. And the contributions on the weekly telephone calls

chaired by Sonny Popowsky and others that have participated have been highly useful and very informative already.

So, with that, I'd like to thank the group, and, of course, attend, as I have the previous calls carefully to the comments of the committee. Thank you all.

MR. POPOWSKY: Thanks, Holmes. Bob?

MR. CURRY: I have very little to add to what you've put together. I think the idea of the descriptive, not prescriptive is terribly important because I don't think the goal of this committee or of the Department to try to line up sort of litmus tests or saliva tests for getting into this whole mix. That's one point. The second point, I would note that, in his confirmation testimony, Secretary Moniz has made this a significant ingredient in the way he sees things playing out going forward. And the fact that it was mentioned in his response to questions from -- I still have trouble thinking about Franken as a Senator, but that's my personal

problem -- in response to a question from Senator Franken, this was a significant part of his answer.

So having a lot of confidence in him and his perspective on our industry, as well as his comprehension of the political ingredients that go into moving things forward, I think that this deserving of the committee's full attention.

MR. POPOWSKY: Okay. Thanks, Bob. Granger, you had your card up first, and then Sue.

MR. MORGAN: Yeah. My apologies if, I should have gotten this to you earlier, but I would like to suggest one additional sentence in section 4. This is a very nice document, I agree with it in its entirety. I would like to suggest we maybe add a sentence that reads, Because the successful adoption of many energy efficiency measures depends on human preferences and behaviors, the EAC believes the DoE would be well advised to place particular focus on the inclusion of high quality behavioral social science in the design, execution and evaluation of at least --

well, of RTT projects.

There is an enormous amount of lousy evaluation and social science that's been done in this phase, I can say that because I have a lot of colleagues who have looked at it, and I think some modest nudge to include some serious social science behavioral design in these projects, not all of them, but at least in some of them, would be appropriate.

MR. POPOWSKY: Okay. Before I move on to other folks, does anybody have any comments on Granger's suggestion, either members of the sub working group or anybody else?

MS. GRUENEICH: Could you repeat again what the proposed addition, and I guess where it would go?

MR. MORGAN: Sure. And you're welcome to edit it. Because the successful adoption of many energy efficiency measures depends on human preferences and behaviors, the EAC believes the DoE would be well advised to place particular focus on the inclusion of high quality behavioral

social science in the design, exclusion and evaluation of our RTT projects.

MS. GRUENEICH: I, maybe eliminate the word particular emphasis. I mean, my only concern --

MR. MORGAN: That's fine, happy to do that.

MS. GRUENEICH: Yeah, because especially for states first starting off --

MR. MORGAN: I can simply say consider.

MS. GRUENEICH: -- confusing what it means to have behavioral sciences included. I don't have -- I mean, I'm all for having better EMND, especially for consistency things like that.

MR. MORGAN: Do you prefer well advised to consider the inclusion, do you like that better? Fine.

MR. POPOWSKY: Okay. Any other comments on -- Merwin, talking about Granger's proposal. Okay, Merwin.

MR. BROWN: Yes. I'm just going to add a vote with Dian, which is, our institution has

also been involved in the human behavior science question, and it is pretty early to make that a hard criteria for something like this. But I do think anything that would encourage that to be brought into the picture would be a good start in the right direction. So, again, I just want to add more weight to what Dian said.

MR. POPOWSKY: Okay. And just to be clear, Granger, you're talking about this, the last page of the document that was handed out under the paragraph numbered four?

MR. MORGAN: I put it at the end of the first of the two paragraphs in section 4, phase -- the paragraph that starts, Under this principle in phase one --

MR. POPOWSKY: Right.

MR. MORGAN: Yadda, yadda, yadda. And then the sentence there. And I'll, I can hand you this.

MR. POPOWSKY: Okay. Are there any other comments or objections or concerns to Granger's -- sure. I think Paul was next, Paul

first -- yeah. I'm sorry, Paul was --

MR. CENTOLELLA: Granger, I appreciate the idea, because I think it's very important that we figure out how to design nudges into the regulatory system, and --

MR. MORGAN: It needn't be nudges, I mean --

MR. CENTOLELLA: I understand that. But, in general, to pay attention to the behavioral economic side of what we do, because we have not paid enough attention to that, and I'm not done seeking you out. I'm a little bit cautious about not also suggesting that, to the extent that there are ways in which this can be done through automation or oh approaches that don't require human behavioral change, that we may be missing an important component, here, and I'm not sure if there's a clear way to integrate that into your sentence.

MR. MORGAN: I'm simply going to add the word often depends on human preferences and behaviors. That's certainly the case. But you're

absolutely right, there are ways to automate or to take people out of the loop, the problem is, in many cases, people are in the loop.

MR. CENTOLELLA: And I guess what I'm suggesting is that it may be appropriate for, if we're going make this suggestion, that we also suggestion that the Department look at ways in which people don't have to be in the loop, or people can be in the loop once and, you know, make a decision that carries forward.

MR. POPOWSKY: Okay. Judith, I think you had a comment?

MS. SCHWARTZ: That actually relates to my question, because when you look at the segmentation and what people care about, and there is a lot of evidence to support that it is really effective, some of the people choose automation. But the idea of choosing to purchase automation is, in fact, a consumer decision. So I guess one of the questions that I have for you, in terms of the scope, that isn't obvious to me as someone new to it is, are you talking about also, are you

including in your energy efficiency and energy productivity talking about price signals, which would be very motivating for some people, and other things related to Smart Grid, which enable the automation to be easily implemented?

Because I think one of the things that's causing a problem today in terms of customer acceptance is this bifurcation that somehow energy efficiency is somehow separate and independent of Smart Grid and dynamic pricing and other kinds of DR.

MR. POPOWSKY: Well, I think the answers, we were trying to be more generic and tried to avoid the pitfalls, I guess, of trying to be too specific on that. I thought that Granger's addition, my own view, it was general enough, and I think what you're saying it was, especially the way you've agreed to modify it, that it would make sense. I have no problem with it, but let me hear from other folks. Sue, did you want to comment on this, too?

MS. KELLY: I would just say that the

decision to automate or the decision to not make a decision is part of human behavior. So that, if you're considering human behavior in constructing these, that's, not participation as well as participation is part of that calculus. So I think it's like Prego, it's already in there. (Laughter) But that would be my comment on that. I appreciate the edits that you've made to address concerns expressed by the group, and I think it is important to try and make sure that the measures that we push forward and try to get states and co-ops and public power systems and tribal utilities to adopt actually are ones that will be accepted by people. That's a great idea.

In addition to that, I would just speak to the overall question that our committee worked very hard on this entire piece, took into account a lot of different viewpoints, we had some nuanced and important discussions among the committee, and I would just urge us to avoid having those all over again here.

MR. POPOWSKY: Okay. Billy?

MR. BALL: Yes. My questions have really less to do with the recommendations in the report, because I don't really have an issue with those. I'm not really going to speak to Granger's comment, I think it's already been talked about. My concern is more of an overall concern in that, as a committee, we're about to officially respond to something that we know very little about. And I just personally don't buy into the account vote for it and then read it. And so I guess my concern is more with the start-off wording where we say that this committee, as a whole, have reviewed the proposal.

Well, maybe we've reviewed what's public, but there's no secret that there's no, there's not sufficient detail to review. And that we fully support this initiative when we don't know the details of the initiative. And I think this is, regardless of the topic, whether it's this issue or any other issue, I just think that's a very strange place for this committee to go to provide verbal input, that's wonderful, to provide

a less formal input is great, I don't have a problem with the input at all. I do have a problem with, at least the way I interpret the opening paragraph, it just seems like a full endorsement of a program that we don't even know the program.

That's really my fundamental question, Sonny, is what, as a committee, are we signing up behind when I don't know details?

MR. POPOWSKY: Okay. If I could just respond. I appreciate that. We did have, we certainly had to rely on the public documents, and there are -- and perhaps the words, you know, reviewed the proposal and fully supports, there may be tweaks to that, but what we support is certainly -- well, I shouldn't say certainly, but I think the idea is that we had, like I said, many meetings over the last few months with input from DoE providing us information that they could. Although, again, we have to rely on the public information. So that we went around the horn several times in our group to say do we generally

support this in principle, and among the working group at least, there was unanimous support in principle.

If it would help to change the language a little bit there to say we've reviewed the public documents related that have been made available so far, and we support this initiative in principle, something like that. I suppose we could do that. Again, I'll look to the other members of the --

MR. BALL: Or to the --

MR. POPOWSKY: -- work group --

MR. BALL: -- we've reviewed, you've reviewed the publicly available information, and you have the following recommendations. I find it hard to fully support something, again, I can, maybe we can get behind and fully support the few paragraphs that are out there, but I just -- I think you're really providing recommendations on the publicly available information is what you're doing.

MR. POPOWSKY: Okay. What about, does

anybody else have any comments on Billy's point -- I'm sorry, were you about to -- did you have a comment?

MR. HUMMELL: I'd like to engage Mr. Ball for just one moment, because, of course, I take incoming from stakeholders all over our field, and have now for months on this proposal. The committee has an opportunity to express to a larger audience that, based on the depth of your expertise and your own interest in the electric power sector, varied as they are around this table, that there is some merit to the federal government giving states an opportunity to be rewarded for superior performance against their own aspirations in areas that are aligned with national interests.

This proposal will not be any further developed unless it is appropriated. It will not be appropriated unless people, in the sector that would have its policies affected by it, find it to be desirable. I cannot be more clear about our constraints and restrictions about further

developing the proposal in the absence of appropriations. I hope that's helpful.

MR. POPOWSKY: Sue, is your card still up? Okay. Wanda?

MS. REDER: Yeah, I support Billy's comments. I don't know if we really concluded on that, but I think the document is well done, and I think with those minor edits, I support.

MR. POPOWSKY: Okay. Bob?

MR. CURRY: Perhaps the way we could present this is, that the committee has reviewed the information that is publicly available regarding the Race to the Top proposal and fully supports the concept as described therein, and has the following recommendations.

MR. POPOWSKY: Billy -- could you try that again, Bob?

MR. CURRY: No. (Laughter) The Electricity Advisory Committee has reviewed the publicly available information regarding the Race to the Top proposal and fully supports this important initiative as described therein. It has

the following recommendations. I'd have to add more words than that, but that's the concept.

MR. POPOWSKY: I'm sorry --

MR. CURRY: Race to the Top concept (inaudible).

MR. POPOWSKY: We can work on the final language during a break, but is that generally where you want to be, is that okay Billy and Wanda?

MR. CURRY: Yep.

MR. BALL: You got it.

MR. CURRY: I hate to agree with Billy on anything, but (laughter) --

MR. POPOWSKY: Whose turn is it? Jay?

MR. MORRISON: Thank you. I also wanted to add support for the idea of the initial sentence going from we have reviewed to have recommendations. There are some things that are in the public documents that it's not clear to me are necessarily exactly consistent with where the recommendations come out. Particularly, I liked very much how Holmes just described this as

encouraging performance, as opposed to encouraging specific policies. I think the lack of clarity of that difference in the public documents is why recommendation to is so good and so important.

And so, because it's not entirely clear to me that the public documents are today consistent with what the committee is recommending, I'm more comfortable with going directly from we have reviewed and have recommendations than we have reviewed and agree and we have recommendations. There's also one other concept that I would love to have seen in the documents, partly just because it's the mantra of our membership, and that's cost effectiveness. We would be uncomfortable if what winds up being some of the proposals that are supported is the replacement of 8-cent power with 12-cent something else. And so, since the President has made a point that Race to the Top should save consumers money, I'd like to see that boiled into the nature of the recommendations, that this is support for cost effective improvements and energy efficiency

and energy productivity, as opposed to leaving that important term out.

MR. POPOWSKY: Did you happen to find a place where you could get that in there, did you, Jay?

MR. MORGAN: Well, you could do it in that first paragraph in section four under the principle in phase one, the Department would provide tools and technical assistance to states and other applicants to help develop cost effective approaches, or their cost effective approaches to advanced energy efficiency, and blah, blah, blah.

MR. POPOWSKY: Okay. That's a good place to put it.

MR. CENTOLELLA: I guess I'm going to voice a different opinion, which is Prego, it's already there. When we say energy efficiency, we say energy productivity, it implies cost effectiveness, we don't need to be adding additional concepts at this point. The commit the worked long and hard to get this language, and I

guess I'm of the opinion we should limit the amount of edits here, because I think it's already there.

MR. POPOWSKY: Good point. I mean, the sentence that Granger just referenced said approaches to advanced energy efficiency and productivity. Is there a subset of energy efficiency that's not cost effective?

MS. GRUENEICH: Yes.

MR. CENTOLELLA: Yeah. I mean, from --

MS. GRUENEICH: Most energy efficiency going forward won't be.

MR. CENTOLELLA: -- LED -- you're really talking about efficiency, and you're talking about productivity, you are inherently making a decision that the value that is being received is in excess of the costs that are being used to create it. If that's not the case, then you're not talking about efficiency and you're not talking about productivity. So I guess I think we're getting caught up in sort of traditional regulatory lingo that I think the approach here was to try to

encourage a broad thinking about how do we move forward on a national energy agenda, and I don't want it to be captured in what has necessarily been the least cost lingo of the past.

MR. POPOWSKY: Jay or Rob? Bob, you still have your cards up.

MR. MORRISON: If the committee believes it's there, and certainly DoE has heard the discussion, then I'm not obviously going to insist. I would like to make the point that I do believe that there is a category of efficiency that is not cost effective, there is certainly a tremendous amount of cost effective efficiency out there to be obtained. But what particularly caught my attention is that the concept of customer-owned generation and efficiency seemed to have been conjoined in some of the materials. And, given that, my concern about cost effectiveness is that much greater.

MR. POPOWSKY: Okay. Well, it seems to me we don't -- okay, anybody else have any, want to put anything else out on the table? It seems

to me that, with some modest edits over the upcoming breaks, we ought to be able to come up with something that we can load on today or tomorrow morning. Hopefully today. Because, like I said, I think it's really important that we put this out there at this meeting rather than wait until October when everything is already decided.

So I guess I would encourage a few folks -- I'm sorry, Pat, did you --

MS. HOFFMAN: One thing I guess I'll just point out to the committee is, I know in past documents, in order to keep things moving and move forward, we recognize that if there was an issue, it was either debated or characterized that we just stick a point note that this was discussed in the meeting, and then leave the document as is. Put a note in the document recognizing, you know, that issue that was brought up so we can just keep moving things forward. We've done that in the past where we've had kind of issues that were kind of debated and discussed.

MR. POPOWSKY: Okay. Granger?

MR. MORGAN: I'm perfectly happy to have the document stay as it is in this respect, but I would point out that a number of folks, ourselves included, in a recent piece in issues in Science & Technology have produced energy efficiency supply curves, and if you go far enough out on those supply curves, it's no longer cost effective. And so that's why I agreed with the comment, but I'm also perfectly happy to accept the language just as it is.

MR. POPOWSKY: Okay. Could I get a few volunteers to meet over the break, Bob, Sue, Paul? Okay. Merwin? Okay. Oh, do you have another comment, I'm sorry.

MR. BROWN: Yeah, I'm sorry. I guess all the comments have got me into a nitpicky mode (laughter). But one thing that does bother me a bit is the statement lifted from the blueprint, it's in number five, recommendation five, as noted in the State of the Union blueprint, the energy efficiency and productivity achievements resulting from the Race to the Top program will not only

save consumers money, but will drive investments that enhance manufacturing competitiveness and improve grid resiliency and cut carbon pollution. Did the committee actually question that, whether those were completely true statements? I mean, I'm not convinced they are. I mean, yeah, I can see instances where this does happen, but I don't see it all following that that will happen.

And I'll just say I feel more comfortable if the subcommittee could suggest that you look at this and were comfortable with those words, and that's okay. If not, maybe just take them out, because it doesn't really add much to the recommendation, per se, as I can see, and neither challenge nor accept that particular statement. But just wanted to raise whether or not you raised the question.

MR. POPOWSKY: Any comments from members of the working group on that? Paul?

MR. HUDSON: Just real quickly. I mean, the reason I didn't raise any objection to that language is because the assumption I was making

going in is that the Department would implement the program in such a fashion as to carry forth those goals. I mean, it certainly all depends on implementation.

MR. POPOWSKY: We could even say, if implemented properly, it would have those results, or we could take it out. I mean, like I said, it's true, the point in that paragraph, like I say, we're focusing on energy efficiency and productivity, but if you really do energy efficiency and productivity, it should have these additional, we agree it should have these additional results. But I have to admit, we certainly didn't do a study of that.

MR. HUDSON: But you see them as criteria as opposed to natural results that would result from any of these activities.

MR. POPOWSKY: Okay. Sue?

MS. KELLY: One possible way to finesse that point would be to move that statement back into the section that describes the Race to the Top section. That way, it's there as a statement

of what was in the blueprint as opposed to something that we all, you know, to a man and woman, all agree 100 percent with. And, that way, it will be in there, but it will be in there in perhaps a less controversial way.

MR. POPOWSKY: Okay. Well --

MS. KELLY: Maybe you could leave this to the drafting group to look at over the break.

MR. POPOWSKY: Yeah. Who have we got on this committee now? Sue --

MS. KELLY: Sue, Paul, Bob, I think, was the --

MR. POPOWSKY: Bob. Okay. Janine, I guess, did you --

MS. MIGDEN-OSTRANDER: I'll help.

MR. POPOWSKY: You'll help too, okay. Janine -- great. Okay. We are just about at the time for our break, is there anything else on this -- I'm sorry, Holmes?

MR. HUMMELL: Before the break, I simply want to express my appreciation to the hard working members of the subcommittee. I first

brought to this FACA a proposal in December of 2012, that was the glimmer in the eye of a budget process that was under tremendous pressure. For the administration to have come forward with a $200 million-plus up to the Department of Energy means that we withstood all comers from all agencies for all time between December and March.

That was an incredible melting, withering assault on our idea, and it was the support of the members of this committee who recognized that there was some innovative potential to refresh the kinds of relations and activities that can take place between the Department of Energy and states and co-ops and public power authorities that gave this proposal the winning status in what is really a fiercely-fought sweepstakes.

To come out of the budget request with this intact is a remarkable tribute to the kind of support that members of the subcommittee have provided in terms of very careful edits, very attentive criticisms, constructive criticisms that

have helped us improve and be more responsive to those in the field that would ultimately benefit from a program if it were appropriated. I won't be here when you reconvene, so I couldn't help but seize the opportunity to express my appreciation and also reflect back to you the effects of your handiwork. Thank you very, very much.

MR. POPOWSKY: Thanks, Holmes, and thanks again to you for all your great work on this, we really appreciate it. Samir, did you have an announcement?

MR. SUCCAR: Just a logistical note. For the break, there is a deli in the building through the double doors and sort of over to your right, you'll see a sign for the cafe, so you don't have to leave the building. For those registered for dinner, we'll have an announcement about that. Dinner will take place at 5:01 North Randolph on the other side of the mall, and we'll have a meet up, we'll announce a time for folks to walk over together, if you so choose.

And, with that, I'll follow up that, the

note about dinner later in the day, but I just wanted to give you those heads up, thanks.

MR. POPOWSKY: Thanks. So shall we shoot for 10 after 3:00, give people 15 minutes rather than just 10. Is that okay, Chris? We'll start promptly at 3:10. We've got a full afternoon ahead of us in terms of the cyber security issues, and then some important transmission issues at the end of the day. So thanks a lot for your attention, and see you at 3:10.

(Recess)

MR. POPOWSKY: Thank you very much. I'm sorry, we're a few minutes behind schedule, but let's get started. Chris, any time you're ready to get started.

MR. PETERS: Sure. Thank you, Sonny. As the agenda indicates, we have what I think is an outstanding panel, with some very distinguished panelists with unique backgrounds here, I think are very germane to the cyber debate that we read about every day in the papers, and hear from the

President and Congress on quite frequently. The title of the panel is Key Federal Roles to Enhance Cyber in the Power Sector. And I can't think of a more appropriate topic, given where we are with NERC-SIP, version 5, and the executive order.

So on my left here, our panelists: We have Marianne Swanson, who is the Senior Adviser for Information Technology Security Management at the Computer Security division at NIST; we have Dr. Robert Coles, who is the Chief Information Security Officer and head of Digital Security and Risk at the National Grid; we have Samara Moore, Director on National Security staff for Cyber Security Critical Infrastructure Protection; and Jason Christopher, with the Department of Energy, who is the technical lead for Cyber Security Capabilities and Risk Management. And Jason, from what I understand, will be taking over the C2M2 model.

So, without any further ado, we're going to kick off this panel with Marianne Swanson, and she's going to give us a couple thoughts on her

role at NIST and where some of her focus is on the cyber debate.

MS. SWANSON: Good afternoon, everyone. I decided I better bring these, just in case, but it looks pretty big at the moment, so I think I'm good. So let's talk about cyber security and what the National Institute of Standards and Technology is doing. So we've been involved in the electricity sector for about the last four years, now. Actually, NIST is also very much, our mandate is to provide guidance to the federal agencies, cyber security guidance to federal agencies. And then, under SSSA, we became involved, then, with the electricity sector.

So, back in about three, no, about four years ago, we started a group called, back then, it was the Cyber Security Working Group, and that was something we put together. Gosh, we had about 800 members that ultimately joined this group. When we formed, when NIST formed and Department of Energy, we formed the Smart Grid operability panel, this committee was brought in under that,

or this working group was brought in under that. So, at this stage, now, the committee, or this Smart Grid operability panel, which is what I chair under the Cyber Security committee, under this Smart Grid interoperability panel has been changed from a member, from a public/private partnership.

So this was a NIST-funded deal, and then the public coming together, we now are a membership based organization. So the SGIP is a membership based organization that started in January. So now we are the Cyber Security Committee under, within the SGIP. So I'd have to say we're having a little bit of, what would you call it, birthing pains, we're coming together, and hopefully, a lot of you are, have heard of the SGIP. And we are now up to about 200 paid members, so we are moving along quite well.

The cyber security committee is doing quite a bit of work, we're continuing on, we're now at about 75 members, instead of the 800 that actually, in all reality, we had probably about 50

that really did work. So now I have 75 that I'm really going to make them work, and they've signed on, so we're going along. So we've been doing a lot. For the last four years, the committee has been quite active, and I thought, well, I'd give you just a few highlights of some of the work we've done.

We put together a NIST interagency report, Guidelines for Smart Grid Cyber Security, in August 2010, and now we're updating it. So this guideline is actually being used throughout, it's global, we've got China, who actually translated it, they're using it, we have the European union, who has taken the recommendations. We have requirements, and they're high level security requirements on the kinds of things you should be doing from a cyber security perspective for securing your information systems, your industrial control systems that are related to Smart Grid. So these requirements are being used in many documents throughout the world, so we really have a success on our hands with this NIST

IR.

Something else that we're working on right now is a user's guide. So we have these requirements and how you should be applying them, but what we really need is a step-by-step very simplistic approach on how you would go about applying the requirements to your system, and walk you through a risk management approach on how to do this. So we're working on that right now. Another document, which I actually didn't list on here that goes with this, is an assessment guide, and it's actually taking those high level security requirements, and how you would assess them, things you would need to look at to see if those high level security requirements were being implemented, thing you should review, people you should discuss, who you should interview, that kind of thing.

So the NIST IR will be updated, it is being updated, we'll be putting it out for public comment, because it is a NIST document, that's the way we do things, probably within the next month

or so. So it's coming out pretty quickly, and that would come out for about a 60-day review cycle. Something else that we're doing under the Smart Grid interoperability panel is reviewing standards. So we have standards, and part of SSSA is to facilitate the development of interoperable secure standards for Smart Grid. So one of the things that we're doing in our committee is reviewing these standards, standards that are being worked on within the Smart Grid interoperability panel, other standards that were deemed key standards that are in our NIST interagency framework document.

So we've already done, in the last four years, about reviews. So we've taken these documents, these standards, reviewed whether they have addressed cyber security appropriately, or, and then make recommendations where we feel that the standard may be lacking, maybe not facilitating the functionality for a secure interoperability. So we have quite a few reviews that have been completed, and these reports are

out there right now on the NIST Wiki site that you can review. So if you're looking at something like IEC's -- gosh, any of them, practically. Pull it up, you can take a look and read it. SEP 2.1 is one we're reviewing right now. I think Open ADR was another one we just reviewed.

So we've got a lot that we've done. And you can then look and see what are some of the security recommendations that we've made and that the standards bodies are now taking back and trying to implement. We've also worked on taking a NIST document, a NIST Special Pub 839, which is risk management, and working with Department of Energy and on NERC to develop a guide for the electricity sector using that NIST document, taking it apart and turning it into something that would be unique to the electricity sector. So we're taking away all that federalese, the normal federal terminology that you get on the NIST Pubs and making it something that's more for the electricity sector.

We're also working on a case study where

we actually are taking that user, that risk management guide and applying it to a fictitious electricity company. So I think it's Papaya Power, and it's quite good, so we're hoping to get that published very soon, because that's a real world kind of implementation of how you would go about addressing risk in your utility. We've also done some white papers, we've taken a look, we actually collaborated with DoE's NESCOR SEP 1.0 and 1.1 mitigation strategy. That protocol had some cyber security related issues and so we came up with ways that you could mitigate some of those cyber security vulnerabilities.

And then, lastly, and there are more, but I'm only going to go on a few, was a white paper on automating Smart Grid security, and this is all about the Smart -- or a Secure Content Automation Protocol, and it's something that we're doing at NIST called SCAP. And SCAP is really the way that we, within the federal government are facilitating continuous monitoring, or situational awareness of all our IT systems. So it's a

protocol where the different tools can talk together using a standard protocol, something that we're very interested in from a Smart Grid perspective. And so we wrote a white paper on that.

And that's just a few. We've done things in privacy that are numerous, as well. So some NIST Smart Grid related projects, so those were the SGIP where NIST is playing a key role as the chair of that committee, but we've also got a lot of, we are doing some things within NIST. So one of them, right now, is we're partnering with the Department of Energy and their Oak Ridge National Laboratory. What we've done is we've taken the NEMA upgradability, AMI upgradability standard, so we've taken that standard and written a NIST IR on how you would test to it. So we've taken the standard and written test cases on how you would test a meter implementation, so an AIM implementation, and how you would test to see if it is meeting that NEMA standard.

And what we've done is, we're now

working with Oak Ridge on implementing that test suite on an actual AIM implementation to see, then, if they, the NIST IR is written accurately from a test criteria perspective. But then, more importantly, to go back to the C 12, the ANCC 12 standards group, who are ultimately going to be revisiting that NEMA standard, to ensure that, when we were testing this standard, what was missing, what needed more work. It would have been nice if we would have tested security in this area, or it would have been great for the standard actually had these things in addition.

So this is a great way of informing the standards body, who is going to be revising the standard, of the additional things that the standard should really obtain. So it's a great project, and it's going along quite well. Another thing we're doing is we're putting to the a test bed at NIST on cyber security. It's a cyber security telecommunications test bed, so that's just getting started. In fact, they're still taking out the walls, so we're not anywhere near

there. And then one other item that you may or may not be aware of is the executive order.

So, back in February, and I know, Samir, you're going to talk about it a little bit more, but back in February, the President issued an executive order on securing the critical infrastructure, the cyber security of the critical infrastructure, and tasked NIST to develop a framework, and we had something like 240 days to do it in. So we have been going, working quite diligently, we've held a workshop just last week -- well, I'll backtrack. We actually, in February, put out a request for information to the public asking, we had about 30 questions on what you're doing, what's important from a critical infrastructure perspective and cyber security, and we received over 260 responses back. Some a couple pages, many in the 20, 30, 40 pages, and some in the 100 pages of responses back to these questions.

So we've taken those, analyzed those, came up with some themes, and then had a workshop

just last week where we had over 420 critical infrastructure participants or stakeholders attend where we went through our analysis of our, of those requests for information responses, and came up with four tracks that we had. And we split everybody up in working groups and came up with the business of cyber risk, the threat management track, a dependency and resiliency track, and then progressive cyber security, or what we like to call it is the basic hygiene and maturity. Anyway, those four tracks were what we were meeting on and delving deep with the members, or with the participants. So now we're going to be having, powwowing tomorrow, actually, and we're going to be developing this framework, an outline, and it will be a fleshed-out outline of what this framework we believe should look like based on the workshop that we had last week.

These themes will come up with best practices and standards, so we'll see. The next workshop is going to be held, and with this executive order, it actually said that NIST, you

must work with the private sector, this isn't for you to go off and do all by yourself. So we're having to convene with the private sector, so we'll be having our next workshop to go over this outline in San Diego July 10th, 11th and 12th. So that will be the next one, and then in September we'll hold the final where we'll have the actual document, the straw man. And, again, everybody will come together, and anybody is invited to look at this straw man and help us finalize it at the very end. So that's kind of the path forward for that.

And then some potential future work. SCAP, as I mentioned a minute ago, is something that we're really wanting to pursue, so I suspect that that will be one of the areas that you'll see NIST delving into. We, the whole lightweight, low power crypto is another one that we feel very strongly that is needed, especially like in the metering, where you want to have encryption, but the devices themselves can't really support that. We also are working with Brazil's Inmetro, which

is sort of a sister agency to NIST, on developing additional AMI security failure scenarios, and then, now, the actual mitigation and how you would mitigate these scenarios, from a cyber security perspective.

And then another one, probably not until the beginning of the fiscal year, but another one we'd like to work with the Department of Energy on would be on supply chain. So I think that's going to come out from this executive order, and all the work we're doing, but this will probably be a gap that we're going to see that we need more guidance in supply chain. So this might be a natural fall out for us to work together on that.

And I think that's it for me, and I guess we're going to do questions at the end, yes? Okay. Very good, thank you.

MR. PETERS: Marianne, thank you. (Applause) And thank you for the outstanding work you've done at NIST and the support you've given the private sector, it's much appreciated. Our next panel list will be Jason Christopher from the

Department of Energy.

MR. CHRISTOPHER: I didn't bring my glasses, but I brought water, which is equally as important for me. My name is Jason Christopher, thank you very much very having me today. I'm not going to be speaking about all of the things that OE does in cyber security, there are a lot, but I will be speaking about the one piece that Chris already alluded that I'll be taking over, which is the Electricity Subsector Capability, Cyber Security Capability Maturity Model, which is a mouthful, so just say ES-C2-M2, makes life a lot easier.

So, to give a little bit of background, this is an administrative-led, this is led by DoE with collaboration from both private and public sector. The challenge was to develop capabilities and manage dynamic threats, to understand the cyber security posture of the grid. The approach that was taken was to actually develop a maturity model in order to measure these capabilities. The results were a very useful tool, and I'll go

through exactly what that looks like, to be able to let a utility sit down, have the discussions and the dialogue, go through and look at metrics to see where you are in terms of maturity for your cyber security capabilities.

The project was kicked off in January of 2012, and by April of 2012, there were 17 pilots, and by May of 2012, the document was released. So, in terms of actually producing something in a quick time span, the team did a fantastic job of giving something that was both timely and useful for industry. The future objectives that we'll be looking at is strengthening the cyber security capabilities. One of the things that I'm emphasize is lot is that we are talking about maturity of the capabilities, and one of the things we're looking at in the future is where is the adequacy and the strengthening, the weaknesses and the prioritization that comes with that.

In order to do that, we need benchmarking. That's one thing that utilities have been asking for, they've been saying, well,

okay, now that I've been doing this facilitation, where do I lie, how do I compare? Those are some of the things we're going to be looking at in the future. And also, with that, comes sharing the knowledge of if people are at a higher maturity, well, would they be able to provide insight and input to somebody who may not be as mature in a certain capability. So, I'm putting some screen, I don't want people to have their eyes glaze over or get overwhelmed because there's ten things on the board. There's a lot.

However, what I will tell you is that, when you do facilitation, we cover all of this in one day. This is very different than other cyber security test audits that are out there which could take on the period of weeks. So, in terms of sort of the bang for your buck, the gut check of where you are, to be able to set aside the time and capabilities for one day and the resources to do this, you're covering these ten different domains. If you talk to your cyber security staff, this isn't going to be anything that is

mind blowing, that seems like a curve ball. It's things like risk management, things that we actually just started, Marianne discussed, that they were talking about for Smart Grid cyber security.

We baked in everything that has been learned from other standards, but also threats and vulnerabilities that we're aware of during the creation of this project. So I'm not going to go through, necessarily, and list all these things, but this is really kind of the basic where you're looking at when you're developing your models and where you want to be for cyber security. So, really quickly, now that you've seen the ten things that we're going to be looking at in terms of domains, where do we rank people. And it's this thing of looking at your maturity levels, the maturity indicating levels, MILs, you have three levels. Technically four, because there's a zero level when you're not doing anything.

In these cases, what you're looking for is whether or not practices have actually been

initiated, meaning that they're on an ad hoc basis. If they are on an ad hoc basis, that would be kind of determined by your resources, who's doing the initiation. So it may vary from person to person if you don't really have a set up, documented practice. So the next part is performed, you're documenting that practice, you've actually done something more than doing the ad hoc, you've had adequate resources applied to them. And, finally, we're talking about actually managing the practices. So you have the documented procedures in place, now you have a policy in place that you can compare to, and maybe you're doing a review cycle on that.

So when we're talking about the different metrics across those ten domains, there are 312 metrics that you're actually looking at. This is what we're ending up trying to find out from what your maturity level looks like. Another thing where -- don't let your eyes glaze over, it's really fun. These are donuts. Everybody loves donuts. The green donuts -- and, I

apologize, I'm color blind, so going forward in the future, I may work on the green shading a little bit. If you're green, whether you've got light green or dark green, it means that you've achieved that MIL. If you see any red or light red, it means that you're not there yet.

And the way that you can see it is in the key right there, on the bottom there; it is fully implemented, largely implemented, partially, or not implemented. This isn't a binary test, there's no pass/fail, if you're going through this and you are, you've got a practice in place, but you have some gaps, okay, well, maybe you're partially implemented. If you've got some things to strive to improve upon, then we could say that you'd be largely implemented. And, likewise, if you've met everything that's in that metric, then fully implemented.

What I want to capture here is something very important, this isn't a one-off test. As you hear, whenever you talk to somebody from cyber security, there's no silver bullet. This is not a

silver bullet, but it incorporates into the practices, it helps you with your defensive posture, it helps you evaluate that. So when you perform an evaluation for the ES-C2-M2, you're going to see where your gaps are, you're going to go back to that wonderful donut diagram, you're going to see where your red pieces are, you're going to analyze those gaps, and then you're going to prioritize.

So if I go back over here and I look at this fictional utility summary score that we would give out at the end of the facilitation, you can see that, for risk, they're at a MIL one, because that donut is all green. But they've got two practices that are not implemented that would get them to a MIL 2. Should they prioritize that, compared to things that are MIL 0, which they're at asset in their cyber security program. Maybe that's where they should be focusing on, especially since you see it's a lightly shaded red, they may be closer to doing that. So it helps with the dialogue to actually figure out

where you're going to prioritize next.

And I also emphasize that, it may not make sense for every single utility to be MIL 3 across the board, this is really something that you tailor to yourselves based on your own internal discussions and on your own resources. So we're not talking about when we say benchmarking, comparing a smaller mini co-op to a larger customer footprint such as a Con Edison, you don't want to necessarily, they're not going to have the same resources at play. So in terms of what your evaluation will look like, it will vary from utility to utility.

Once you prioritize and plan out how you're going to implement something, you can then implement to fill those gaps, and then, finally, really encourage everybody to go back and perform the evaluation again. It doesn't necessarily have to be an annual basis, once again, this is tailored to what you would want to do, but it would be shorter or longer than that to find out where it is that you're tracking along and how

you're getting there. One of the things that we encourage people to do before facilitation takes place is actually figure out where do you want to be, or where do you think you are right now.

The dialogue of where you think you are, and then you do an evaluation and you find out where you actually are, could spur a lot more internal dialogue about where you want to be later. A lot of that's an educational for utilities that have participated. I'll get back to that in one second. So one of the things I want to talk about also is kind of the usefulness that utilities have seen in this. So far, since the pilot programs, we have had roughly a dozen or so self-facilitations where we actually go out to the utilities and help them with facilitations at no cost. We've had over 200 people request the tool to use for their own purposes, so it has gained traction, we are looking at more people who want to do this kind of life cycle analysis of where their cyber security capabilities are.

Lastly, what I'll leave with -- and I

realize that there's a lot of information, so I will be here and entertain as many questions as people can throw at me. I want to give you a real life scenario of when the team had put together why you'd have these different ten logical domains, what they were there to address. They are to address real threats. There was an APT, an Advanced Persistent Threat, discovered by McAfee in 2011 called Night Dragon. So Night Dragon used social engineering techniques, combined with well-coordinated targeted attacks with Trojan horses and other malware, so when you look at how that is being reacted to, you can then see where you'd want to be with this model, and why the model would end up helping that. So social engineering.

And one of the things that the practice in the ES-C2-M2, one of the metrics is having the awareness based off your own threat profile. So, with that being said, if you're getting a phone call that says that I'm from IT and I need to know your password so that I can update your account,

maybe one of the things you bake into your situational awareness is that IT will never ask you for your password. It's things like that that kind of start the dialogue, and so that's captured in the work force domain. Likewise, you have very simple things like known vulnerabilities and lack of awareness, information sharing, being a part of the ESI set, getting their alerts, ICS or US-CERT.

So all of this is kind of baked into the model, is what I'm trying to get at, and it's based off of real life things, it's not sort of an esoteric or existential exercise, there is tangible results that can be played, here. With that, the model is online, it's really available. If you e-mail ES-C2-M2@DoE.gov, the e-mail goes to me and my team, we will happily answer any questions you have on it. Likewise, we provide the tool kit, which is more than just a model that you see online. The tool kit itself will give you the lovely donuts when you fill out all the questions, so you can find out how much green or red you have in your donuts.

We provide that so you can go off and do your own facilitations, do your own life cycle analysis, but, again, we offer these free facilitations, we'll go out and we'll help you do the exercise itself. Thank you very much.

(Applause)

MR. PETERS: Thank you, Jason, and I'm sure all of us will never eat Dunkin' Donuts again without thinking about cyber, so thank you. Our next panelist is Dr. Coles from National Grid. I've had the privilege of working with Dr. Coles for two years, he is the founder of the North American Chief Information Security Officer Forum that he founded two years ago, and marshaled industry leaders across the utility sector to talk about subjects such as cyber threats, risk, NERC CIP, and he's done an outstanding job at leading this forum and helping us.

He has brought some of his best practices from the U.K. over to the U.S., and I find it ironic that somebody from the U.K. had to form a North American alliance to get us all

moving in the right direction.

So, with that said, welcome, Dr. Coles.

DR. COLES: Thank you, Chris. Chris asked me to talk about a real life case study of (inaudible). So, just a little bit of context for those that don't know, National Grid operates in the U.S. and the U.K. In the U.S., in the Northeast, we deliver and transmit gas and electricity for quite a big chunk of the Northeast, and all the generation for Long Island. In the U.S., we're the monopoly transmission system operator for electricity, and we transmit and distribute gas to about a fifth of the country, about 8 million customers in the northeast of the U.S., and about 18 thousand staff, so I think we're the second, I think we're still the second biggest investor and utility in the U.S.

So that's the context. So, in terms of enterprise security management, everything we do is driven by risk. My team is dedicated to risk management, so we have a systematic process of

looking at threats, looking at incidents, understanding the business and how it's changing, which may introduce risk or it may mitigate risk in its own right. Similarly, technology and technology changes, which, again, new technologies may introduce risk or may, indeed, mitigate risk. And then compliance, which is driven by legislation and regulation.

So those are all the things that we look at when trying to understand risk, internal and external, or they provide us with an independent view of all of that as well, which goes into the formula. And then the outcome of that formula is our understanding of risk, and if we think that the risk is too high, given our risk appetite, and that drives the program for the things that we do to reduce risk. Otherwise, then, we're happy to look at the risk and accept it, put it on the risk register and regularly review it.

So that's what my team does, in the bottom left hand corner. I joined the organization three years ago from the financial

sector, I was Chief Information Security Officer for Meryl Lynch before this job. And I guess the trigger for change for us was that my boss joined the organization, he's the CIO about six months before me, he was expecting to see -- he came from finance, Thompson Reuters, and I think CIO for the Royal Bank of Scotland before this, and various other bank jobs. He was expecting to find a big, complex cyber security team with the senior person having it out, and he just didn't find that, he found a very small team, half a dozen people, low level, very buried, very far down within the IT organization.

So his challenge to me was to build a team, which we've done over the last three years, to getting on for 14, my team now. We cover governance, risk and security within IT within IS, investigations and threat management, I've got a group that are specialists, security subject matter experts which get involved in all the systems change and systems development we undertake, making sure that when we buy or when we

build systems, we ask for security and we get what we ask for. I've got a group responsible for strategy, architecture and policy, a group to face off against the businesses so that we can articulate technology risks to the businesses in such a way that they fund, where appropriate, the changes we need to reduce the risks, and then a very small privacy team.

We built a risk management and reporting structure around the activities that we undertake, so we have committees in the U.S. and the U.K. because our businesses are quite separate, they are run semi autonomously. We have regional security resilience committees which look at all the risks and make the decisions about the appetite for risk, and then they report up into a global risk and business risk. And a resilience committee that reports through to the exec and through to the board. So I get to address the board roughly about twice a year, the full executive committee roughly three or four times a year, and on a monthly basis the U.K. and the U.S.

resilience and security committees.

So that's the overall structure. When I joined the organization, the challenge from my boss was to answer the question, how secure are we. Very large, very complex organization, very difficult question to answer, actually. The way that I chose to do it was initially through a whole series of workshops, so I ran 33 workshops covering all business areas, all asset types by getting together business people with IT people, with risk people, with audit people, and we brainstormed the threats, we brainstormed the vulnerability of those assets to those threats, we brainstormed the current level of control, and then we looked to see if there were any gaps and what we could do to close those gaps.

That was actually quite a cathartic process for the National Grid, nobody ever got some of these groups together before, and we found that individual people had worries and concerns that they've never been able to tell to get on the table. We found that individuals had part of the

picture, but actually had never spoken to some of their counterparts that had the other part of the picture. So actually getting people together was quite a good sort of cathartic process, and doing it in a bottom-up way also got the buy in for the things that we needed to do and the momentum to really carry the program forward.

We looked at the threats to the National Grid, we conceptualized the threats in two ways; we conceptualized it in terms of causes and effects. So causes or the threats, we look at malicious actors, and we look at benign factors which could give rise to threats. So the malicious actors, we look at foreign nation states looking to steal intelligence for espionage, the gain or benefits of companies operating in foreign countries. We look at rogue actors, rogue nation states looking to cause damage, we look at criminals, criminals looking to steal data information that could give them financial advantage.

We look at terrorists and radicalized

insiders that could look to cause damage internally with their national grid, people who we employ, or contractors or third parties. And then -- so that's the threats. If you look at the outcomes or the impacts, then we track the two main risks that we have, which is a catastrophic cyber security breach of critical national infrastructure systems. So that's really the systems that run electricity and gas, essentially. And we look at the (inaudible) sub security breach of business systems and data. So, without the National Grid business systems, it's going to be very difficult to operate the critical national infrastructure systems, because there's a dependency there.

And then a new risk that we haven't really fully got our heads around at the moment, which is IT embedded in operational technology. So this is something that's really crept up on us over the last, sort of 10, 20 years, really. And the equipment that we use out in the field 100 years ago would have been all mechanical, 50 years

ago it was electromechanical that would serve as motors and analog systems controlling that. And, slowly, over the last 10 or 12 years, it's slowly being converted to essentially PCs and servers. So you buy a substation these days, and, essentially, you're buying a data center, a fully fledged, fully equipped IT data center with modern technology in it.

We've got a lot of legacy equipment in National Grid that's been built up over that period when we weren't really sure, I think historically, what we were buying. And, to be frank, we didn't ask for any security because we didn't realize that it needed it all those years. So this is something that sort of crept up on us that we're giving quite a lot of attention to at the moment, just to try and understand what that risk is and what the size of that risk is. That's led to the overall program of investment. So the improvements that we've made over the last couple of years, and we continue to make, we're investing in end point security, shared information, network

security, access control and some specific improvements in those systems that run the electricity and the gas networks.

And that was spread over a number of programs and foundational things that we just needed to get on with and do quickly, make some improvements in, and tactical things which were short term, but which really gave us a measure of protection while we were building a bigger strategic, long-term remediation program. That program is about half way through at this point. We're tracking the risk production, we got the joy of doing the workshops, so that very granular level, of course, is where a huge amount of data, so we can very finely track the risk reduction that we get through the entire program.

We recognize that we are not an island -- clearly we're an island, the U.K., within the U.S. We recognize that we work with other organizations, as Chris kindly mentioned, I've been trying to convene my peers and get some of my peers together to work cooperatively together. I

find that very useful as a check and balance on what I'm doing, and hopefully, others find the same. So we share information amongst ourselves about threats, about our programs, about what we're doing.

I think we do need better intelligence and coordination from the intelligence communities, we're quite good at sharing information ourselves, but we don't have access to that intelligence community readily. It's a little ironic, my English accent, so clearly, I'm a foreigner. My boss is a CIO who is a foreigner, his boss is the CEO, he's a foreigner, so the three people that could actually spend money based on intelligence given to us, we're not allowed to know, because we're foreigners. So I have to have my staff security cleared in the U.S., and they're not allowed to tell me some things, but, you know, it's not an ideal situation, but we get by.

We need disruptive capabilities, we, as a commercial, as a private organization, we can't disrupt criminals, we can't go out and attack

people, it's against the law, for one thing. So if we're being attacked, we can defend ourselves, but we can't respond or retaliate. We do need a regulatory environment that allows us to invest nimbly in security, the threat is changing very rapidly in cyber security. So when I joined the organization, there were very, very rare the reported incidents, very, very few cyber security incidents. We're now finding that we are regularly under attack, as are our peers, and that's regularly being reported in the press, as I'm sure you all see.

We need, we do need a regulatory environment that allows us to very quickly react and direct our investment dollars to defending ourselves, which we don't have at the moment, I don't think. And we do need facilitated coordination of incident response across government and business. And that exists to a certain extent, and I think the Obama Executive Order will certainly help to improve that. What we don't need, we don't need forced disclosure of

incidents, because that in and of itself can lead to us disclosing vulnerabilities that other people can take advantage of.

We don't need more standards, audits and compliance-based rules, we've got plenty of those through NERC CIP. Ironically, historically with the National Grid, that's actually led to us holding back investment in some areas because where NERC CIP defines that we must do certain things to protect the bulk electric system, then historically, management have said, well, if that's what FERC and NERC requires, then that's the minimum, then that's also the maximum, that's the only thing we'll do. So, historically, those standards have actually held back investment for us.

And, finally, sanctions for infringement of the rules don't help, either, so where you're forced to disclose incidents and there's sanctions for not doing so, you tend to find that lawyers crawl all over everything before anything can be released, because it must be declared by a lawyer

incident. So, again, ironically, where you're forced to disclose incidents, actually, in some respects, it limits the amount of information that's disclosed and actually reduces information sharing rather than increasing it, in some respects.

So that concludes the thoughts I have. Chris?

(Applause)

MR. PETERS: Thank you, Dr. Coles. And, lastly, we have Samara Moore from the National Security Staff.

MS. MOORE: Thank you. Good afternoon, all of you. So I am the one at the end, and the one with no slides, so I hope to keep you engaged. So I appreciate the opportunity to talk with you a little bit this afternoon about the White House's efforts related to critical infrastructure cyber security. At the White House National Security Staff, I'm on detail for two years, or a year and some time, and my role is Director of Critical Infrastructure Protection, and given the activity

that we have going on right now, my main role is the White House lead for implementation of the executive order. So I am living and breathing it right now.

So I wanted to talk to you a little bit about that, and really, the combined approach that's being taken to address the cyber threats that are faced by the critical infrastructure, really focusing on the combination of information sharing and adoption of cyber security practices. So, first, to start out, a little bit about the cyber security challenge that we are faced with. As organizations realize the efficiencies from information technology, we're seeing increased reliance on information systems and the internet to accomplish core business functions or to achieve mission objectives.

A good example of this is grid modernization, that's definitely leveraging technology, but we're also seeing that it is opening up to new threats that, really, we haven't had to focus on or deal with before, and these are

threats that need to be managed. So the trend that we're seeing is, and you guys, I'm sure, have seen articles in the paper on this, or even heard speeches and presentations on this, but we're seeing that threats are continuing to increase in intensity, and increasing in complexity, but also the skill set required to be able to carry out such attacks is not as high as it used to be. We're seeing that the accessibility of tools and resources to carry out some of these attacks is much more open and available than it used to be.

Also, we're seeing that the impact of the cyber threats is on, could be potentially on your reliability, right. So there may be concern of impacting productivity and performance, but we're also seeing an impact that may not be immediately apparent, and that's a concern that we're very much aware of, related to economic impact, and that's on our intellectual property. So, as we're working on innovative technology and ways, we're really concerned about our intellectual property, theft of business-sensitive

or proprietary information, as well.

So, to address these concerns, one of the activities that the President is focused on is the Executive Order. And, as Marianne mentioned, in February, Executive Order 13636 was signed, and the intent, the goal was to help strengthen cyber security protections for critical infrastructure. The Executive Order is designed to increase the level of core capabilities that our critical infrastructure has in place to be able to manage these cyber threats that are faced, that we're faced with. And it does so by focusing, really, on three key areas; the first of which is information sharing, the second is adoption of core cyber security practices, and then the third is insuring that all of the actions done in this space are done with strong consideration and protections of privacy and civil liberties.

So we see a clear role for government in increasing cyber protections by sharing and leveraging those unique resources that the government has to partner with critical

infrastructure owners and operators in managing cyber threats. And we're doing that now, there are existing programs in place to do that now, but we want to do more of it. In particular, if we talk about information sharing, over the years, there are several programs, we take for example both within DoE and within DHS in sharing information, we've shared lots of technical information, threat information. What we want to do, though, is do more of that, we want to do a better job of that.

And so, we are working with the information, the intelligence providers to make sure that we're getting information out to critical infrastructure stakeholders in a timely manner and in a manner or a way that's useful to you, and to the degree that we can provide information at an unclassified level, we're trying to do much more of that in a useful way. Not to state that we don't recognize the need for clearances, and so expediting the provision of clearances is part of the activities within the

Executive Order, as well, and DoE and DHS specific to the electricity or the natural gas sectors are currently working on processes for that.

We also, as I mentioned, are committed to making sure that we address privacy and civil liberty concerns, in particular as it relates to information sharing, privacy and civil liberties is an area that represents a challenge that has to be addressed for us to be able to share information to the degree that we should, that we really need to, to impact this problem. And so DHS has the lead in working and coordinating with the agencies to make sure that privacy is addressed. And then, finally, we're working with the private sector to develop a framework of core practices to really, again, work to develop these capabilities, those core set of practices that all organizations should have in place to some degree to manage cyber risk.

Underscoring this framework, and it was mentioned in the remarks earlier, is really a recognition of the need for cost effectiveness,

and making sure that, in this framework, it's considering cost and the impact on owners and operators, and also looking at practices that are flexible and scaleable and can be applied to different organizations based on their organizational context and their risk profile. So Marianne gave us a description of the framework and the process that NIST is going through to develop it, from our perspective, and NIST is working really hard to do this, the framework really should leverage existing industry best practices and guidelines in this area, where appropriate, and incorporate those core security measures.

What I'm referring to are these common industry practices that many firms are doing already, either in whole or in part across the organization. A great example of this is the ES-C2-M2, the capability maturity model that Jason just briefed us on, which really, I look at this body, it really leverages a lot of work that several organizations here participated and

engaged in and helped us to develop. In particular, the framework, you know, there's concern on how does this impact existing requirements and regulations. The framework is not focused on compliance, however, we're working really hard to make sure it doesn't undermine existing requirements that are in place.

Also, as we go through the development process, we recognize we may identify gaps where further work is needed, and we may have recommendations for standards bodies to develop either standards or guidance in these areas. We also understand that, with the framework, so what we're focused on is addressing a significant part of where we're being impacted by cyber threats. We realize that the advanced attack or the persistent attacker or the well resourced and well funded attacker may still be able to get through. Because, again, what we're talking about is cost effective flexible core practices.

However, what we want to do is reduce the noise, we want to address those core areas

that all organizations should be, again, in a cost effective and risk based way. That way, we can focus our efforts on the more sophisticated threats, but then also it causes the attacker to have to focus their efforts and work harder. The last point that I want to make related to this is, is that we're well aware of the interdependencies across sectors, and we're looking across the critical infrastructure community to have a consistent risk based application of cyber security risk management.

We see that this is particularly important, you know, coming from DoE, my focus has really been on the energy sector. Now that I'm looking at all 16 critical infrastructure sectors, I constantly hear and I constantly see the significance and importance of interdependencies. So this is something we're also paying particularly important too (sic). So, the impact on this body of all the activity I just described, I'll sum it up in a couple of bullets. One, information sharing. There's sharing going on, we

already have examples of where we're starting to improve and increase those processes for this body, and I encourage this sector to continue to be engaged and take advantage of that.

There's information sharing forums such as the ESISAT, ISC-CERT, the DHS in-kit, those are all resources that are available now, that the sector should be leveraging. And hopefully, what you'll see is continued improvement and refinement in information sharing there. And then the second area for this group is adoption of practices. Many of you are doing some really great things in this space, I've worked with you guys or with folks in your company, I really encourage you guys to continue to partner with us as we develop this framework. We really want to get it to something that is usable and implementable and could really achieve the objectives that I stated earlier.

So moving away from the EO just a bit, I want to talk just a second on legislation. We recognize that the Executive Order is not enough, there are some real challenges that we have.

Particularly, we mentioned information sharing, that could only be addressed through legislation, so we're continuing to actively work in this area. As it relates to information sharing legislation, there are three fundamental priorities that we're focused on. The first is carefully safeguarding privacy and civil liberties, insuring that we preserve the long-standing and respective roles of mission, and missions of civilian and intelligence agencies, and then provide for targeted liability protections to help enable information sharing.

It's important to note that, on the legislative front, information sharing is not the only part of what's needed, there are other areas that we're also looking for to be addressed in cyber security legislation. So, again, continuing on with the theme of promoting adoption of cyber security best practices, updating the laws that relate to federal agency networks, and then giving law enforcement the tools that they need to fight crime in the current age, and creating a national data breach reporting requirement.

So, in conclusion, you know, I'd like to reiterate that we're really focused on partnering with critical infrastructure stake holders with owners and operators to work together to manage the cyber risk. It's really about risk management. And we continue to promote an understanding of the threats that are out there, but not just the fact that there are threats, but really making that link between the business and mission functions, the organization's objectives in the cyber threats, and making sure that we understand what those impacts are so we can make informed risk management decisions and investments in cyber security.

So, thank you, and I look forward to additional questions. (Applause)

MR. PETERS: Thank you, Samara. What we'd like to do now is open up the floor for the committee members to ask any questions that you may have based on our panelists' briefings this afternoon.

MR. POPOWSKY: Chris, I think Pat wanted

to make a couple comments.

MR. PETERS: Okay.

MS. HOFFMAN: You guys are going to have to indulge me on this one, because I'm passionate about this subject. First of all, one of the things that we've been driving for and towards is a risk based process, and so we had did a risk management plan with the electric sector, really looking at the governance structure, which goes back to how does a utility look at their enterprise system and evaluate risk. Because the first thing you're going to do is really understand the risks, or your perceived risks.

Now, in my conversations with folks is, not everybody interprets risk the same way, or has a high or low tolerance for risk. So if you don't start at the right level of what do you perceive the risks are and your acceptance level of risk, I think, especially with the conversation with the regulators, you've got to get on the same page of -- because you're not going to be 100 percent secure. I mean, the investment that's required

can, you know, get exponential as you get less and less risk tolerance, and so we're going to have to figure out how to work that conversation, at least to get folks on the same page on the risk analysis, at least a governance structure.

I was very appreciative of the conversation of having somebody in charge of cyber security, from National Grid's perspective, but that's one thing to look at as we move forward. The second thing is, when we -- so once you go from the risk process, then it's going down to evaluating your maturity level. And the reason that we pushed really hard on maturity level, went back to the question of how secure are we. And, in my mind, when we were having this conversation, it was like, what capabilities do we need to have in the industry to demonstrate that we have our arms around cyber security. And it was a way to say, okay, confidence level, if we're secure, we have a good understanding of maturity around cyber security, we have good situational awareness, we have a strong idea of what the threats are, we

have role based access, these are all confidence, but maturity level in which we hope to guide the conversation.

So one of the things that, when we looked at the maturity model was a way for everybody to focus how they would represent how secure are we. Because I get that question all the time, and it would be nice of the community to figure out or think about how do we all answer that question in the same way, and what are some of the metrics. I have situational awareness tools, I can have, I have visibility over my system, different things, I have role based access, so we can kind of go through the process of at least representing how secure we are the same way. I mean, I'm interested in National Grid's perspective on that.

The other question or the think that we looked at with respect to capabilities, and I know it's not ideal, but we looked at kind of the physical maturity model that some people will have developed, and it was done under DHS, but when the

conversation becomes more sophisticated, the security experts are able to sit down and say I know the cost effectiveness of a camera versus a fence versus a guard dog, and they can put a weighted kind of assessment of cost effectiveness around those different tools. And one of the things is, we've got to get to that level in the cyber area where we can kind of compare capability A versus capability B, and say, okay, the security guys feel that having this type tool is a little bit stronger than having B, and it helps us with that overall long-term investment strategy.

So, as I look to develop, or as the industry looks to develop best practices, one of the things that I'm keeping in the back of my head is, really, a little bit of a weighted evaluation on some of those different best practices for cost effectiveness and performance, so that as people go forward and say, okay, how do we invest in it, we can have a little bit of a baseline. Supply chain, gosh, that's a big issue, and these guys can comment, but the frustration thing there is,

there's a lot of vulnerabilities out there, how do you prioritize it. The cyber community, if a vulnerability isn't fixed because they perceive it's a higher risk than the supply chain developer, then they disclose the vulnerability and they write an exploit on it, and they put it on the internet. And, God, we need some better kind of, how do I say it, morals or something in the R&D community, supply chain community.

And the question that I have, is there some need for disclosure roles within the supply chain community and the users, even if it is directly between those to disclose any vulnerabilities as they're discovered so that the utility or the users can better assess their risk. Because it's hard for a utility entity to assess a risk if they're waiting for some third party R&D organization or cyber organization to disclose it on the internet, and then have to back it up into their processes. So something to think about, I wouldn't mind your thoughts on that. But determine practices really come into play, there.

So I guess the last thing that is, I met with several CEOs, with the Deputy Secretary, senior leadership of DHS and DoE, and we've been talking around this subject for a while on priority, and I guess we put a little bit of a stake in the ground saying, okay, out of all the domains of the maturity models, what would be the three top things that I would want the industry to focus on in the near term. And the first one was situational awareness and the development of situational awareness tools. Because what we don't know is hard enough as an industry, and so we need to, there's publicly available, commercially available tools out there that provide great insight, so as a community, as an industry, it's how do you want to have the tools and who needs to have higher sophistication in tools versus some of the basic tools that are out there to gain more situational awareness.

So situational awareness, some people call it continuous monitoring. I use those terms interchangeably and I probably shouldn't, but so

that's priority one. Priority two goes back to what Samara talked about Merwin's talked about it, is information sharing, making sure that the information is shared between like entities, so IOU to IOU, and regionally sharing of information because something may be seen in one utility in the Washington, D.C. area may be seen by others. So how do you create a forum where you can share information. But also between the federal government and industry, back to what Samara said, and making sure it's actionable, and how do you do care lines and the architecture to make sure that it's actionable.

The third thing is actually running through incident management, but really going through and taking a look at the exercises that are out there and making sure that we have some procedures in place to manage incidents. The thing that we're going to have to get sharp on real quick is how much, how many resources do we need in looking at forensics analysis or looking at other support infrastructure to manage a cyber

incident. So that's another thing that I've asked the community to take a hard look at, and relate that to exercises. So I just wanted to put that on the table of what some of what's being remarked on. And I guess the last point is our high factor R&D activities.

What should we be working on that, I'll say disrupt them, but I don't think it's, for cyber security, everything's armor plating it. If it's anything, it's what type of approach should we look at with how we're operating the system, what insights can we gain from sensors and separate data measurements, characteristics on the system to have redundancy and have the ability to represent the security of the industry.

So I'll leave it at that, but I just wanted to add that to the conversation.

MR. PETERS: Thank you, Pat. Robert, any thoughts on a couple of themes Pat touched on?

DR. COLES: Is that good, okay. Yes, you mentioned processes of risk assessment, risk management, I completely fully agree with that. I

find the current regulatory structures we have around NERC CIP really pull directly against that. It's, within National Grid historically, it's held us back from looking at the risks, it's given us a false sense of reliance that if it's mandated by NERC, if it's within the set standards, then that's both the minimum and the maximum that we must do. And if that's mandated, then that must be good for us, therefore, we'll not bother to do anything else.

So you talked about minimum standards and what everybody's doing, that's really on the control space. What we kind is that you can't benchmark risks because the risks are completely unique to National Grid. The impacts to us if National Grid goes down, the threats to us, there may be some commonality in the threat, but certainly, the impacts and the probability of attack are completely unique to us, you can't benchmark risk. And, therefore, I really quite strongly agree, I strongly would like to suggest that the role of the regulator should be around

assessing the proficiency of the organization around understanding its risks, and then managing those risks, and then challenging the controls decisions. And then as they go around lots of different organizations in the country, normalizing and saying, well, if your peers are doing that, why are you doing that.

And then you can have a grown up discussion with the regulator and you can say we're not doing that because we're managing our risks, and that risk, we don't need to do that because we're managing that risk in a different way. And I think the current regulatory structures that we have don't facilitate that conversation. They're very black and white, and it's very much down to if it's mandated in NERC CIP, you must do it, and if it's not, then nobody does it in the industry.

MR. PETERS: Thank you, Robert. Bob?

MR. CURRY: Who's running this meeting?

MR. POPOWSKY: Yeah, right. Chris, do --

MR. CURRY: Robert --

MR. POPOWSKY: -- you want to take the questions and --

MR. PETERS: Yeah, go ahead, Mr. Curry.

MR. CURRY: This is Bob Curry, former regulator in New York and I'm quite familiar with your activities both in that state as well as New England. And I look at the New York staff, which is good sized, 565 or 70 people, but the folks who are assigned this task are nowhere near as, how shall I put it, up the learning curve as you all are. So when you're relating on the distribution networks, you're dealing with the states as opposed to the transmission that you deal with in the U.K. and the transmission you deal with here.

Do you think there's adequate education at the regulator level, is that something that the DoE might be able to enhance and give you folks that you can have the all the conversation you alluded to with, because they have matured a great deal in a short period of time thanks to education?

DR. COLES: Yes, I do, and I'm doing the best I can to educate, certainly, the state level, I'm seeing Masti Eudora Friday, actually. And your PSA do have got a good understanding at the state level of cyber security, and they've recently conducted an exercise to look at strategy, cyber security strategy, which was a very thorough review. So I think it's patchy. Yes, absolutely, I think there's a need to increase the level of skill within those organizations.

The difficulty, I guess, would be how do you recruit senior expensive experts into an organization like that, how do you keep them busy, how do you give them a career path, how do you keep them. So I guess, realistically, they could be brought in from consultancies and from external organizations, I guess, is the issue with that.

MR. CURRY: Or, maybe in New England, we could get Gordon to socialize the cost. He's not paying attention, but -- (laughter)

MR. PETERS: Yeah. We've got a question

from Granger.

MR. MORGAN: Yeah, actually a comment and then three points. I mean, my principle concern in this space is the reliability of the bulk power system. And the problem is, of course, we have to take the problem, think things apart. I mean, cyber security also applies to smart meters. I don't much care, personally, although I understand that, if you're trying to collect bills, you do care about hacking smart meters, their reliability of the financial and billing systems.

And unless they're interconnected to the SCADA in some way that they shouldn't be, that's not likely to cause problems with the bulk power system, that's going to be similar to the sorts of problems that all major firms face. So let's stay focused for a moment on the bulk power system. And so my first comment is, we need to be really careful not to get overly fixated on cyber attacks on the bulk power system at the expense of physical attacks. I mean, I don't know how to

bring the power system down for weeks and weeks or months with a cyber attack, I know how to do it easily with a physical attack, and so one does need to keep some since of balance.

The second comment is that, I understand all the reasons one needs to put more and more intelligence into the bulk power system, that is more control, more real time automation, more autonomous agents, and so on. But every time I do more of that, I presumably also introduce additional vulnerability in terms of places where a smart attacker can get access. And I have not been able to figure out how to do a balancing analysis. I mean, I've been trying to figure out how to do this, because I train doctoral students in this sort of space, and we just produced a lovely PhD, for example, looking at the question if I could cycle hundreds and hundreds of smart meters that are frequency, that is critical as a resident frequency of the bulk power system, could I do any serious damage. You can't prove a negative, but we don't think the answer is yes, we

think probably you can't.

But I don't know how to work that broad of a problem, so if any of the four you have any insight about that, I'd sure like to hear it. And then the last thing I wanted to ask about is red teaming. Who is actually trying to figure out how to make attacks that will bring down the bulk power system, get to the point of just not quite pulling the trigger, and what empirical evidence is there that a higher maturity score actually provides greater protection against that?

I mean, I understand that maturity scores are lovely, but can I have confidence that, because I have a high maturity score, the effort level for a red team attack on my bulk power system will be much, much greater than if I have a lower maturity score? It's not clear to me.

MS. SWANSON: I can talk a little bit about maturity and then I'll definitely hand -- little bit about the maturity and then you can, by all means, since that was a document that I wrote many, many years ago under NIST, was a maturity

model using, actually, Carnegie Mellon's, the CMM maturity model, so it's kind of interesting. I think what it does show is a basic level of improvement over time, so you shouldn't be taking just one snapshot when you're looking at the maturity level, you should be looking at it again to see if you're improving.

MR. MORGAN: And we're talking just about bulk power here?

MS. SWANSON: Well --

MR. MORGAN: I understand about billing systems and all the other things, but we're talking just about bulk power?

MS. SWANSON: Right. Well, I don't think that's just about bulk power, I think it's about your whole organization, because ultimately, that does affect power, is your organization's view on cyber security, as well. So there's a lot of program management pieces to cyber security that need to get deployed, and that starts with work force and goes on from there. That, ultimately, will affect bulk power, from a cyber

security perspective, so I think it's a lot of things, it's not just the technical, and we get it, ICS and SCADA is very not, in a lot of cases, not IT. But there are a lot of pieces to it that are not just technical, so you've got your operational and you've got your program management pieces. So I would say yes.

MR. CHRISTOPHER: So, as I said before, it's not a silver bullet, I don't want somebody to take the ES-C2-M2, or any maturity model, period, and think that if they applied this, they're going to have the answer. What it does do is it gives you indicators. So, one example, I'll take the risk of naming an example really quickly. Just the risk domain, so -- is mine on? Hello? Am I closer? There, we go, I'll just put it right there.

So, the risk domain is an example. One of the things it asks about is whether or not you do risk assessments, whether or not you have risk models. There are a lot of risk models out there, you can find, you can just Google right now,

anybody that's got a computer, risk models, you're going to find hundreds of them. There's no way in the model, there's no, it's agnostic as to which one you would pick. So I want to go on a facilitation and attack what risk model you ended up choosing and saying that, well, you shouldn't be doing that, you should be looking at this other one.

It's not about the adequacy as much as it is are you having the conversations, are you doing ad hoc risk management process or are you actually having documented procedures in place, do you have a policy, even, doing an annual review of, do you have the resources kind of dedicated towards that? It's the first step of the conversation, so it's not the time end-all, be-all, this will get you to security, it's the evaluation of whether or not you're having those types of conversations.

So, to -- and I've got the four other things, here, I took notes during your questions, so I can get to all --

MR. MORGAN: I was asking, are we running closed loop? That is, are question doing red team attacks on the bulk power system --

MS. MOORE: I can talk to that --

MR. MORGAN: -- confirming that higher, you know, scores on maturity lead to a greater effort at attack.

MS. MOORE: So, I can talk to that, as well, as part of the team in the development. And one of the key, a couple of the key inputs into the development was leveraging some analysis and work that had been done over the years, very similar to what you were referring to. So there's a program that does, I believe it would be considered red teaming, for selected entities and where very skilled professionals perform analysis of an environment ahead of time, and then they go in and try it again and see what they can do.

And that had been done over a period of time, and we leveraged the recommendations that came from those types of exercises and incorporated that into the practices, as well as

some vulnerability testing and work that had been done by the National Laboratories, and then the common recommendations that had come from years of doing vulnerability testing on industrial control systems. So consideration for that was a significant input, along with some analysis of threats and vulnerabilities in that space. And so, as Jason said, it gives you indicators, but what we found from both the results of the red teaming and some of the common vulnerability analysis work were there were similar capabilities that would address those cyber threats, and that's what has been incorporated into the model.

MR. MORGAN: Okay. So I'll shut up, but I think I've just heard the answer, we're running open loop in this space.

MR. PETERS: Thank you. I think next question, Phyllis, thank you, you had your hand up.

MS. REHA: Yeah, thank you. I'm looking at this from the state regulator's perspective, and Dr. Coles mentioned as one of the needs is a

regulatory environment to allow investment in security infrastructure to address changing risks, and you have to be nimble and be able to do that quickly, and that we don't need more standards or compliance-based rules. So I'm thinking about that from a regulator's perspective that has to review those infrastructure costs, or cost recovery, and we have to do an analysis of cost effectiveness and cost benefit analysis for that cost recovery, and if we don't have standards to guide that analysis, how do we judge the cost recovery?

So I was just wondering if you would address this kind of broader policy kind of issue, as opposed to some of the technology issues that were raised.

DR. COLES: Yeah, sure. So, I think the way you address it is by evaluating an organization's processes for understanding its risks and challenging its decision making processes, and then doing exercises like the New York PSC has done recently, which is to go and

review every single utility in the state to look at all their practices, and then to normalize and say, well, if all of your peers are doing this, why aren't you doing it, and then you can have a grown up asking with your regulator and you can justify not doing that, because you're doing something different that's better or because the threat isn't the same.

And I think you do it through evaluating those processes of risk assessment and risk management, challenging those processes, and then by doing that lots and lots of times across the whole geographical area and getting an understanding of what everyone else is doing, you can act as a normalization agent.

MR. PETERS: I think Paul had the next question.

MR. CENTOLELLA: I guess I want to, I'm troubled by something that I've been troubled about for a long time, and I'm troubled a little bit by some of the comments in this discussion. There were a couple of comments about, well, we

can't expect every organization (inaudible) to be doing the same, have the same capabilities, be making the same investments. But that strikes me as something that is not a risk based criterion. I could imagine a small utility that, if it was vulnerable, could potentially do real damage to the interconnected power system.

I'm interested in your PhD thesis, Granger, about whether or not those sites can do damage to the power system. I am concerned, when I look at the NERC CIP standards that there are, that even in CIP five that smaller generating plants are at the lowest level of requirements. I'm concerned that, you know, only aspects of the distribution system are even included within the bulk power system's definition, and therefore covered.

And I'm wondering has anyone really done an analysis to ensure that what we're looking at in the area of cyber security, that what we're evaluating governance on including all of the right things that actually represent potential

vulnerability to the bulk power system.

MR. CHRISTOPHER: I guess I'll lead off with, when -- and I made a similar comment regarding the capability and maturity model, that maybe not everyone would want to be at a certain level. You're right with regards to the vulnerabilities, but when you're talking about the risk, you're talking about the vulnerabilities and the impacts. So it's more than just the vulnerabilities by themselves, the risk equation itself is vulnerabilities, impact and threat.

So, depending on the utility's risk profile, they'll have to internalize that themselves, find out, okay, what are our vulnerabilities. And some of them will be common, you're actually right, their control systems have commonalities and they have common vulnerabilities, same thing with IT systems. But they also may have a different threat profile and they also may have different consequences.

To your point regarding the size thing and whether or not you're looking at different

loads, again, with risk, what you would be looking at is communications and how, in a cyber environment, everything connects. So it wouldn't necessarily be, well, I have this much load and therefore, if I lose this, it will have this much impact. It's more about, if I lose the system, if I lose the communications between the systems, what is that consequence. Because that's more of what the cyber security attacker would be going for, is to cripple those -- and I know that systems, I'm not talking about distribution or transmission, I'm talking about, for example, like your e-mail system or your communication system that you rely upon.

So when we talk about different risk profiles, you're really looking at a broader picture than maybe just your generation facilities or your customer load or what type of fuel type. It's not really based off of that for the cyber security elements of the risk part. Does that make sense?

MR. CENTOLELLA: I'm not --

MR. CHRISTOPHER: I see your face --

MR. CENTOLELLA: No, maybe I haven't been clear about my point. So if I'm talking about critical national infrastructure, here, I'm not talking about the billing system. I could imagine a small utility with a critical facility in a critical location that, if it came down, would not just affect that utility, but would affect the interconnected grid, as a whole.

MR. CHRISTOPHER: Right.

MR. CENTOLELLA: And, so, I am wondering whether or not we are setting up criteria in how we think about this that does not reflect the risk to the system as a whole, and how do we insure that there's not a gap in our governance in an organization that maybe is a small utility that maybe doesn't have a lot of resources, but if we looked at it from a national perspective, might be critical to the maintenance of the power system.

MS. MOORE: Yeah, so I can talk to that point. So one of the activities that we do have underway, DHS is leading in partnership with the

sector-specific agencies is looking at each of the sectors, so electricity is part of that, and understanding what are the critical functions within the sector, then understanding for each critical function what's the value chain, and then what are the systems that underpin that, so then we can identify and understand what organizations own and operate those assets so that they are aware, or their impact nationally.

So, at the start, so that's what we're calling it, it's a sector-level risk assessment process that we're going through for all 16 sectors. So, at the start, we're focusing on catastrophic impacts, catastrophic national regional impact to public health, public safety, national security and economic security. That will be completed by July, that is a very high threshold when you say catastrophic. From there, we'll look for further analysis, but we started with the highest threshold and we're continuing to work through that.

So there's some sectors that are further

along than others, but we are at least doing that initial catastrophic assessment, and then focusing -- we're not limiting our efforts to only those, but we want to have awareness and make sure that they are aware, so that we can manage that risk. It doesn't mean that they're not already managing the risk, but just making sure that we understand where that lies. So that is something that's currently underway.

MS. SWANSON: I guess I'd like to add to that. So, part of that piece that they're talking, that she's just talking about is going to be put into the framework, as well. So it will be something we're calling a filter. So as we come across and start to develop this framework document on best practices and providing guidance on how the sectors should be securing their IT and their OT, we'll be using that as guidance as to how we put that together. So that's a piece of it, as well.

MR. PETERS: Thank you. Let's go to Commissioner La Fleur.

MS. LA FLEUR: Thank you. I have two questions, if you will indulge me. My first is for Robert and your comments on regulatory standards. I do understand your point about the compliance overhang and the concern about compliance-based standards and the need to have a risk-based process. But I'm interested in your explaining the point that any standard that sets a minimum will automatically become the maximum. Because, under the scheme in the Federal Power Act that we're required to implement with these consensus-based standards that are drawn from registered entities, large and small, across multiple sectors and regions, you're necessarily going to get a consensus-based standard.

And it's certainly not the intent, for example, in a tree trimming standard that whatever the envelope defined in the standard is the maximum, and you could never trim your trees more, and will go on and say no, you must trim to only that. And I'm interested in why the minimum becomes the maximum.

MR. COLES: It becomes the maximum because, if you don't have an educated set of management that really understand the risks, then they don't engage in that deep thinking about what they're protecting themselves against, and therefore, they assume that if this is the consensus of the industry, well, that must be good enough for us. And, therefore, the actual tendency for uneducated management is to say that is the maximum that we will do because that's what the industry has opined on.

Now, it works really well for tree cutting, because the risk, the threat for tree cutting, the threat for overhanging branches on the power lines hasn't changed in the last hundred years, we've got some really good statistics on it, we know really finely what the threat is, we know clearly how, if you cut back to a certain degree, then the probability that some damage will be caused to a line is reduced by a very precise amount. In this area where the threats changed since I've been in the industry, three years,

significantly, you can't afford to wait three to five years to gain industry consensus because the threat you're addressing is three to five years old.

And, therefore, the money that you're spending on that three to five year old threat isn't the current threat, and it's diverting resources away from what is the current threat and defending yourselves against the state of the nation today.

MS. LA FLEUR: Well, that's, obviously, really an argument against using the whole NERC-based consensus standards for cyber security, which this is probably a segue to my next question, but some of the Congressional things we've seen would have a whole different way of determining cyber security standards and so forth, but if, in fact, as -- I know you're right, that the risks change quickly, that makes it even more unfortunate if a standard that might be a couple years old becomes the maximum. I would that management would think, well, there might be

places we need to go beyond because the risks have changed.

My second question is for Samara, and I completely understand if you can't answer it, because I say that all the time when people ask me questions. But I share your hope for legislation that helps address the information sharing even more than the Executive Order already did, because we need to get the information in the hands of people who can act on it. And I'm curious whether, as you look at, we've seen so many pieces of legislation kind of bubble up by committee, get passed by one branch and not the other; is it your, do you only accept multi sector legislation that takes a comprehensive look at this, or is there any openness to energy-focused cyber security legislation?

Assuming that all the other privacy and civil liberties -- and I realize I'm not asking you to endorse any specific bill, I'm just curious, because we've seen a lot of energy-specific pieces of legislation sort of seem

to start to move, and I don't know if that's a nonstarter, if you can say.

MS. MOORE: So, it's not something that I can really speak to. I do know that we're open to discussion on different areas, but it's not something that I can speak specifically to.

MS. LA FLEUR: I understand. Then I'll take that as a comment rather than a question, thank you very much.

DR. COLES: Could I come back just on the point I made earlier? Sorry, just one further point. I think there probably is a medium ground, here. If you look, if you compare other regulatory regimes, if you look in the banking sector, particularly at Basel II, for example, there's a two-tier regulation. If you have a very simplistic understanding of your risks, if you're not sophisticated, if you're a small organization, then it allows you to follow a standard, just apply the rule, apply the standard and that's good enough.

If you can demonstrate that you've met

them all, that you've had a challenge over your thinking about how you understand risks, you've got a sophisticated risk management process, and you can prove that to your regulator, then you get into a different sort of regulatory regime, you get into a different conversation. So I think there's probably a medium ground looking at a different sector, which seems to be, seems to have worked reasonably well. Certainly last to lead, if not from three, four years ago.

MR. CURRY: Could I just jump in for a second? Going back to Commissioner La Fleur's comment, one of the concerns that I had is for state regulatory agencies who are charged with looking at the prudence of expenditures, often the minimum can become the maximum if they are -- that's why I asked the educational question earlier, if they're not far enough up the learning curve, the accountants will come in and say, hey, you exceeded the minimum, that's on your shareholder's equity side, it's not on the rate payer's side. Have you run into that at all?

DR. COLES: I have, and I've overcome that through talking about the risks and through educating management about the risks. And the risk of not recovering that money that we're spending is a risk that they're prepared to take, because they think it's important enough to manage the risks.

MR. PETERS: We'll go to Ralph.

MR. MASIELLO: A little discomfort, I'll raise this question. Samir, you had supply chain, I think, and I think you also did on the DoE donuts. The dominant scape vendors are global firms that develop software around the world. Most of the other places that develop software are in the European union, therefore, plausibly no worse than domestic, but historically, they've had software developed in places like Moscow and Singapore.

So, and then, second, it's common business practice in that industry to deliver the source code with the system. It's usually a contractual requirement. And even if the U.S.

Operation is not selling systems into Libya or Jordan, European businesses are. So here we've got critical infrastructure, and chances are good the source code for a lot of it is sitting in places that you wouldn't let a U.S. supplier sell the stuff to. And this has been a rant of mine for some time, that we focus on intrusion and external threats, but the threat of something buried in three or four million lines of source code, sitting there for five years, is probably the greatest threat, and certainly the place where the damage potential is the highest.

So, and it's also the case, if I, as a contractor, want to work for Gordon and get into Gordon's facility outside visitor quarters, I'd probably have to go through a background check, but I can get a job writing software for a scape vendor without that. So, to me, there's a supply chain problem, here. Now, maybe this has been addressed in the past couple of years, and I'm on a rant, but I don't think so, I think the risks in the supply chain are much greater in many ways

than we realize.

MS. SWANSON: I guess I'll attempt. Yes, it's scary, there's a lot of potential places where bad things can happen to your products. It can happen from the software, it can happen from being sitting in a warehouse after the product has been put together and something getting put in there, there are a lot of places where the integrity of your product is vulnerable. And we're aware of that. So NIST has written a special publication on supply chain that talks about the kinds of things you, as a procurer of products, should be thinking about and what you can put into your procurement language.

And, yes, and I'll tell you, with the vendors, we've had an uphill battle trying to get this, the first draft even through because the vendors are saying it's impossible for them to do these things, that they have vendors themselves or product suppliers and they could not do these things, and request this. And I think we have to change that mentality, we have to start to demand

that we want good source, we want good, secure code.

We have ways to write it, we know this, there's a whole software assurance group in DHS that is part of this, there's another group out there that does this for Microsoft, so there are places where we're starting to do this, but it's not an easy one, I'll guarantee it.

MR. MASIELLO: I think I have to join Granger's company, then, in assessment. A second question that's related to it, and I'm not going to describe the way I would modify a scapetive system because irreparable physical damage, but we're not, to my knowledge, doing anything on resiliency where another piece of the interconnected IT systems can detect that something that shouldn't ever happen is happening, and stop the process.

We're worried about the security and the intrusion and validate the data exchange from a protocol standpoint, but not from a realized that you're being told to do something you shouldn't.

I mean --

MR. PETERS: Okay. Samara, I'm going to have to keep this on track, so this will be the last response.

MS. MOORE: Okay. I'll keep it brief. So, there definitely has been some discussion specific to that, both considering cyber physical and not looking at each in a vacuum, but considering cyber physical as well as what you just discussed. So one of the approaches that both the Executive Order and the Presidential policy directive that was issued at the same time does, is we transition to take looking at things from a cyber physical perspective, as well as not focusing on critical infrastructure protection. But now you hear us saying critical infrastructure security and resilience.

And so one of my key partners in crime at the White House is my peer on the resilience side, and so now we're working rather closely together to look both at security and resilience, and really trying to have the appropriate balance

of protective measures, detective measures so that we can identify when things go wrong, and it may be identifying something on the physical side that doesn't quite look right that might be an indicator of a cyber or vice versa, and also response and recovery capabilities.

So we're starting to approach this challenge from a different perspective to take into account what you've addressed, which has come up a lot in our discussions.

MR. PETERS: Okay. Again, a round for the panelists, thank you. (Applause)

MR. POPOWSKY: Thanks, Chris, and thanks for the excellent panel, we really appreciate your time and thoughtfulness. Why don't we move right into the last subset of our agenda today. Gordon van Welie is going to pinch hit for Mike Heyeck, who was unable to be here today on behalf of the Transmission Subcommittee, and they have a couple orders of business to take care of before we finish today.

MR. VAN WELIE: Thanks. Yeah, I was

kind of hoping to run on another 15 minutes. And let me say up front that if there's any glory to be had today, I'll take it, and if there are any complaints, we'll send them to Mike, how about that? So I'm hoping this will be reasonably brief, there are two decisional items and two updates for the committee. The two decisional items, the first is a paper with a recommendation on the future of interconnection wide planning.

And I think the best way of teeing this up is to quickly read to you two paragraphs that are at the beginning of the document, which both summarize -- well, it's a summary and a recommendation. The EAC commends the interconnection-wide planning efforts to date funded by the DoE. This funding provided the first of its kind interconnection-wide planning efforts in the eastern interconnection, and both of the existing interconnection-wide efforts in the west and Texas. The process allows for greater stakeholder input across governmental and private sectors.

The EAC recommends that DoE work with each group to facilitate their continued efforts with clear objectives and governance and assist the groups in arranging their own funding mechanisms either through established mechanisms, by proposal to the DoE, or by other means. To the extent that other funding is more forthcoming, we encourage DoE to protect the rates of substantial return on its initial investment by responding positively to well grounded proposals from the interconnection-wide planning groups.

So I'm not going to go through the rest of it, I'm hoping everybody's had a chance to read through this, but it's a fairly simple recommendation and I invite discussion. And, Sonny, when you're ready, to take control of it.

MR. BALL: I'm actually fine with what the paper says, participated in that group. I guess my only additional comment, Pat's here, and other folks, I think one of the key items here is, as we move forward, all of these processes and groups, we need to, our long term focus needs to

be moved into an area where these good efforts are sustainable on their own.

And I do fully agree with the recommendation of the paper, but I would just encourage DoE, if you do continue to fund certain aspects, always ask the question, do you have a plan -- you know, this doesn't go on forever, the authorities asking do you have a plan to where you can get yourself to where your efforts, your involvement are self-sustainable in some way. Because I believe they can be, and I believe in these efforts.

MS. HOFFMAN: Billy, I would agree with that. I also recognize that we tried models that had success, and, you know, there's areas of improvement. And one of those things is, you look at sustainability as we continue to find ways that really makes it effective in how these sort of interactions occur. So, from that perspective, I agree wholeheartedly.

MR. POPOWSKY: Any other comments? We've got a motion to support the recommendation

from the Transmission subcommittee. Wanda moves, is there a second? Becca? Great. All in favor, say aye.

MULTIPLE SPEAKERS: Aye.

MR. POPOWSKY: Any opposed? Great. That wasn't so hard, Gordon. (Laughter).

MR. VAN WELIE: Great.

SPEAKER: Excellent, Gordon.

MR. VAN WELIE: Okay. I'll take the glory on this one, thank you. So, the next one, I might be deferring to Mike, we'll see how this one goes. (Laughter) So this is a recommendation on the CSG interstate transmission signing compact, and I've had occasion at the break to have some offline conversation with Dian and Tom, and so I've got some words missing that I would like to propose to the Committee. Let me just explain the context before I jump into some of the details, here.

It seems like there are some concerns about the details of the interstate electric transmission line signing compact, and there was

also references in the paper that NARUC had considered this, and apparently, they have not yet. So we need to correct that. Clearly, Congress contemplated their states could enter into interstate signing compacts in order to deal with transmission. So the thing I've attempted to do in my wordsmithing is separate that source, the fact that Congress encourages states to consider interstate signing compacts, and still retain what Tom would like to see the committee do, which is to provide some level of support to the specific interstate signing compacts that's attached as an example to this particular proposal.

And, so, really, the recommendation is then framed as asking the Department to engage in supportive efforts as are reasonable, including but not limited to communicating to state governors and legislatures the DoE's support for the state's adoption of interstate compacts in general, sort of interstate, small I, small C, but including as appropriate the specific interstate compact that is referenced in this document. And

then, furthermore, to advocate for the adoption of compacts, and that would be compacts in general in regularly scheduled DoE NARUC's discussion and DoE's technical conferences.

So, really, just to repeat sort of two thoughts, separate answers thought that we'd like the DoE to be supportive of compacts in general, and that, where appropriate, in other words, in the right forums or the right space discussing this specific proposal, be supportive of this proposal, as well. And so, if you accept those two basic thoughts, there are probably a couple of dozen edits that have to be made to this document in order to conform the document with those two thoughts.

I can walk you through them in detail, or you can just leave it up to me to do it, and I'll take some direction from you on that.

MR. POPOWSKY: Tom, you want to --

MR. SLOAN: While I obviously would like a strong a statement as possible, because I do think that it does help the Department and the

FERC meet some of the objections raised to what's in EPAC 05 in terms of backstop, signing authority and transmission quarter designations, and all. I also recognize that there are concerns from the regulatory perspective, even though this is voluntary, states don't have to participate and utilities don't have to participate, but Gordon showed me the conceptual language and would be caveat that I would like to see the final version from Samir, I can support the proposed changes.

MR. POPOWSKY: Okay. And I know, Dian, you had some questions about this.

MS. GRUENEICH: Yes. I want to thank Gordon and Tom working with me on it. I'm comfortable with the changes. I mean, my particular concerns are having been involved in the area of both state regulation and transmission for 20 years, now, very detailed. When I think about the role of DoE -- first of all, the role of this advisory committee to DoE, and then the role of DoE going forward, I become very worried that it backfires for DoE to be going to states saying,

okay, this is how to solve your transmission problem, here's the compact that has been developed, and now go ahead and use it.

So this approach, I think, is a little more nuanced, more falls in line directly from Congress saying we endorse the use of the concept of the compacts, so I think it's appropriate, then, for DoE, in the various forums, to say, we agree with that, as well. But, again, it's a little more nuanced by saying in a particular situation, it may be where the states themselves sort out the specific compact approach, which this one could well work, but maybe there's some different approaches. So that's sort of what I think would overall be a better role for DoE to be taking with regard to the states and why. I think it's been for us giving advice to DoE what I tried to add to the discussion.

MR. POPOWSKY: Rebecca?

MS. WAGNER: Thank you. First I wanted to -- I've been back and forth on this issue, and before the language change, I wouldn't have been

able to support it, not because I don't support the concept of it, and this is why I wanted to, why I'm making a comment now. I like the idea of state compacts, California and Nevada have a state compact on Lake Tahoe, it's survived over many years, so I like the idea of it. What I've been concerned about with this compact is, one, I'm not sure I agree with the interpretation with respect to EPAC 2005, to me, that went more to the national interest court orders designated by DoE as congested areas, and would only those states be part of a compact. So that was unclear to me.

It also suggested, not that every state is not doing enough for transmission, and I would argue that states in the west have been. States in the west probably wouldn't use it because they probably wouldn't be able to figure out how to get along with California (laughter). So I didn't want a one-size-fits-all approach, but, to me, it's a great tool for the tool chest. So, with these language modifications, I can support it.

And I love the concept, I don't think it

can apply everywhere, but I think that certain states, it could be very valuable.

MS. KELLY: I'm just raising a point of procedure. You all are talking about language changes, but we haven't seen them, so are you going to give them to us before we vote on this?

MR. VAN WELIE: We keep this deliberately away from you so that -- I'd be happy to sort of just walk you through my proposed changes. I wanted to first have some discussion on the general concept, otherwise, the discussion on those specifics is kind of pointless.

MS. KELLY: Okay. That makes sense to me, I just thought I was going to hear all of a sudden, and now let's vote, and I'm, you know -- I wanted to make sure that I'd like to see some words before we do that.

MR. VAN WELIE: Okay. Sue, you're holding my feet to the fire. So --

MR. CURRY: Point of order, Mr. Chairman. Would it be more propitious to try to do a turnaround over night and take a look at the

exact language in the morning?

MR. POPOWSKY: Yeah --

MR. VAN WELIE: Because, Gordon, I've seen him type with two fingers, I know he can do it.

MR. POPOWSKY: Yeah, and hopefully, our -- Samir and the --

MR. VAN WELIE: Yes, that's exactly what I was thinking.

MR. POPOWSKY: But I think you gave us -- hopefully, I haven't seen them either, I think we've all got the concept, and then when we turn it around, we can, we have a lighter agenda tomorrow, so I think we should be okay tomorrow to do that, as well as the Race to the Top changes, which we made a lot of progress on today, as well. But we can talk about that in a few minutes. But is that okay, Gordon, can you work with Samir and get that --

MR. VAN WELIE: Yeah, because I think it would be good to, if we can, distribute it electronically so everybody can get to see it

before we, rather than listening to me read it out.

MR. POPOWSKY: Right. Do you want to -- so we'll hold off on any vote until tomorrow. Gordon, you had a couple of other transmission subcommittee things you want to report on.

MR. VAN WELIE: Yes. There were two on pace, one's really brief, it says here status in the paper of the transmission technologies. My understanding there is that that's on hold until we hear back from the DoE grid tech team, so we'll come back to that during the course of the year. And then I was going to ask David Till to give us an update on the status of work on grid resiliency and ageing transmission assets. So, over to you, David.

MR. MARCHESE: We have two major sections that have been drafted, one on the ageing assets of the grid, Clark Gellings, and the other reasonable solutions by me. We'll be combining those, making sure that we're consistent, and then the rest of the paper, we'll build from there.

And we're planning on coming back, I believe, at the next -- I may be mistaken, but I think it's the next EAC meeting that we'll be presenting that.

MR. POPOWSKY: And at that next EAC meeting, I believe is when Mike has planned, Mike Heyeck has planned to put on that panel and some of the post-Sandy related issues.

MR. MARCHESE: Yes, that's correct.

MR. POPOWSKY: Are there any questions or comments for Gordon and David or Clark for the transmission subcommittee issues? Okay, good. Thanks Gordon. So tomorrow, then, we will have a revised draft of the transmission compact letter. We've taken care of, now, the interconnection-wide planning, and hopefully, by tomorrow, we will also have a revised draft of the Race to the Top letter. We made some progress on our short meeting this afternoon at the break, I think we just have a couple more issues to iron down. If I could just get those little subcommittee members together at the end.

Not the little members, but the little subcommittee (laughter). And, otherwise, thank you very much, and I think Samir will now tell us when and where we're having the members -- I'm sorry, one other point. And for those of you who are still in the audience, if you, the comments from the public are to be made at the end of the day tomorrow. And if you do have any comments, any issues you want to raise with the committee, please register them with Sherry or Samir so we know that you want to speak tomorrow, and I'll ask again tomorrow to see if there are any public comments at the end of the session.

So, Samir?

MR. SUCCAR: Okay, great. So, on dinner, for those that are registered for dinner, the restaurant is call ed Tutto Bene, it's at 501 N. Randolph, and if you have any further questions about dinner or the location, you can ask Sherry -- Sherry, raise your hand -- and she can help. We're going to walk over with a group at 5:40, the dinner is at 5:45, and starts with some

refreshments.

So, if you have any questions either on what entree you ordered, walking directions, or any other specifics, please see Sherry. Thanks a lot.

MR. POPOWSKY: And where is the group leaving from at 5:40?

MR. SUCCAR: Right here in the lobby, right by the front doors.

MR. POPOWSKY: Okay. So if anyone wants to join the group, that's fine, or you can head on over there on your own. Does anybody have anything else before we adjourn for today? Okay, good. I hope many of you can join us for dinner. Thank you very much.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

COMMONWEALTH OF VIRGINIA

I, Carleton J. Anderson, III, notary public in and for the Commonwealth of Virginia, do hereby certify that the forgoing PROCEEDING was duly recorded and thereafter reduced to print under my direction; that the witnesses were sworn to tell the truth under penalty of perjury; that said transcript is a true record of the testimony given by witnesses; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this proceeding was called; and, furthermore, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

(Signature and Seal on File)

Notary Public, in and for the Commonwealth of Virginia

My Commission Expires: November 30, 2016

Notary Public Number 351998

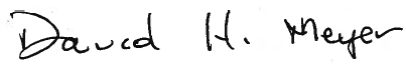
Respectfully Submitted and Certified as Accurate,

Richard Cowart
Regulatory Assistance Project
Chair
DOE Electricity Advisory Committee

9/10/13
Date

Irwin "Sonny" Popowsky
Pennsylvania Consumer Advocate
Vice-Chair
DOE Electricity Advisory Committee

9/10/13
Date



David Meyer
Office of Electricity
Designated Federal Official
DOE Electricity Advisory Committee

9/10/13
Date

Matthew Rosenbaum
Office of Electricity
Designated Federal Official
DOE Electricity Advisory Committee

9/10/13
Date