UNITED STATES DEPARTMENT OF ENERGY

ELECTRICITY ADVISORY COMMITTEE MEETING

Arlington, Virginia

Thursday, September 14, 2017

PARTICIPANTS:

NOHA ABDEL-KARIM
North American Electric Reliability Corporation

JOHN ADAMS
Electric Reliability Council of Texas

ANALEE ARMSTRONG
S&P Global Market Intel

MELODY BALCET
AES

VENKAT BANUNARAYANAN
NRECA

LANEY BROWN
Concentric Grid Advisors

GIL BINDEWALD
U.S. Department of Energy

CAITLIN CALLAGHAN
U.S. Department of Energy

CECE COFFEY
ICF

LOUISE FICKEL
U.S. Department of Energy

TRAVIS FISHER
U.S. Department of Energy

ANTHONY GRIECO
Cisco

STEVE GRIFFITH
NEMA

PARTICIPANTS (CONT'D):

JOE HENRY
Deloitte

ARTHUR HOUSE
State of Connecticut

PAUL HUDSON
Osprey Energy Group

LAUREN ILLING
BCS

CARL IMHOFF
Pacific Northwest National Laboratory

KATIE JEREZA
U.S. Department of Energy

HENRY (HANK) KENCHINGTON
U.S. Department of Energy

MLADEN KEZUNOVIC
Texas A&M University

JOYCE KIM
U.S. Department of Energy

BARRY LAWSON
NRECA

KEVIN LYNN
U.S. Department of Energy

LARRY MANSUETI
U.S. Department of Energy

JOHN MCILVAIN
U.S. Department of Energy

DAVID MEYER
U.S. Department of Energy

PARTICIPANTS (CONT'D):

JEFF MORRIS
Washington State House of Representatives

DAVID NICOL
University of Illinois at Urbana-Champaign

ROLF NORDSTROM
Great Plains Institute

PAUL PARFOMAK
CRS

MELISSA PUALEY
U.S. Department of Energy

CHELSEA PELLECCHIA
ICF

THERESA PUGH
Theresa Pugh Consulting, LLC

RICHARD RAINES
ORNL

JAMES REILLY
Reilly Associates

MATT ROSENBAUM
U.S. Department of Energy

JAMIE SHIMEK
PNNL

PAM SILBERSTEIN
National Rural Electric Cooperative Association

ALISON SILVERSTEIN
North American SynchroPhasor Initiative

RAMTEEN SIOSHANSI
Ohio State University

PARTICIPANTS (CONT'D):

JOSHUA SMITH
ICF

JULIE SMITH
U.S. Department of Energy

BLAKE SOBZAK
E&E News

ANGELA TROY
ICF

DAVID WADE
Electric Power Board of Chattanooga

WENDY WALLACE
Deloitte

TOM WEAVER
American Electric Power

LORNA WISHAM
First Energy

YILONG XU
ICF

* * * * *

P R O C E E D I N G S

(8:00 a.m.)

CHAIRMAN ADAMS: I'm John Adams and if we all find seats, we're going to get ready to reconvene. You know, one of the things EAC does at their meetings now, they always have a safety tip at the beginning of each meeting and usually I look at those and just go oh yeah that's -- okay. I do want to point out that these decorative stones that are put into the sidewalks around Washington, D.C are much slipperier in the rain than the concrete pavers. That's my safety tip for the morning, having ice-skated here from Holiday Inn.

Boy, we're all set up, bright and early. We're going to start out with a panel on cyber security organized by the Smart Grid Subcommittee and Laney Brown is going to serve as our moderator this morning. So Laney, if you could kickoff.

MS. BROWN: Thank you. So thank you for the Committee and also for the panelist in joining us. I think that both this Committee and the

public, generally speaking, are increasingly aware of the growing risks of malicious attacks. Generally, and obviously specifically focused on our power system over the course of the last, I would say, three or four EAC meetings, this continues to be a discussion point and as we were discussing yesterday in particular, the growing need for increased connectively and censoring and monitoring and that distributed intelligence on the grid really only increases that potential risk and impact from cyber attacks. In January the EAC heard presentations from the Internet of Things and I have to say my memory, if my memory serves, they're really dire warnings of the risks created by the IOT network and that connectivity. And then yesterday we talked about the need for cyber resiliency, so a very, very relevant topic today. We'll continue that discussion with four experts who are strategically thinking about and addressing these issues.

Before I introduce the panelist though, I do want to acknowledge the work that Paul

Centolella has done in coordinating this panel and I also want to recognize Josh Smith's efforts in helping also -- well, me in particular kind of stepping in and preparing for this meeting.

So to introduce the panelists, Carl Imhoff is the Vice Chair for Great Modernization Lab Consortium and the Manager of the Electricity Infrastructure Sector for the Pacific Northwest National Laboratory (PNNL). He manages the Electricity Infrastructure Research Program and in 2014 was selected by DOE as a Laboratory Chair for the Department of Energy Grid Modernization Laboratory Consortium with -- as we have discussed to some extent yesterday.

David Nicol is the Franklin W. Woeltge, forgive my pronunciation, Professor of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign and Director of the Information Trust Institute. He is PI for two recently awarded National Centers for Infrastructure Resilience, so very relevant from our discussion yesterday. The Department of

Homeland Security (DHS) funded Critical Infrastructure Reliance Institute and the DOE funded Cyber Resilience Energy Delivery Consortium (CREDC). He is also PI for the Boeing Trusted Software Center and the National Security Agency (NSA) funded Science of Security Lablet.

Anthony Grieco is Senior Director of the Security and Trust Organization. Mr. Grieco leads the Trust Strategy Office and responsible for Cisco strategy to provide security and trust to countries as they look to digitize key industries in government. Anthony is also responsible for Cisco's security and trust efforts related to IOT.

And lastly, Arthur House became Cyber Security Risk Officer for the State of Connecticut in October of 2016 and recently completed the Connecticut Cyber Security Strategy. From 2012 through 2016, he was Chairman of the Connecticut Public Utilities Regulatory Authority. He has extensive experience both in the federal and private sector with federal experience in the Office of Director of National Intelligence, the

National Security Council, and Staff of the U.S Senate, and in the private sector including senior positions in manufacturing, insurance, and banking. So, obviously clearly qualified participants and we're going to start with Carl. Thank you.

CHAIRMAN ADAMS: And while Carl's getting up there I'm just going to mention there are bios out on the desk outside; very worthwhile to pick up. Thank you.

MR. IMHOFF: Okay. Right button, correct? I'll scoot this way. Well, I'm not able to --

MS. BROWN: It's the art and the science part.

(laughter)

MR. IMHOFF: What am I doing wrong here? There we go. Okay. Well, good morning everybody. It's a pleasure to join you. I'm amazed with how many of the people on the Committee now we've actually worked with back over the years; there are a few new faces in the room. It's an important

time and I think it's appropriate Laney given that you're from New England, all you see now is you have a Nantucket sleigh ride which is you know from the old New England whalers, they put their harpoon in the whale, they'd lash the rope down to the boat and they'd hold on for dear life and hope to hell they were on top of the water when the whale got tired. And that's kind of the way I feel if you look back at the last 20 or 30 years in terms of the utility activities. Profound change, we have over 2,500 synchronized devices at the bulk power system where we'll pass

percent on AMI, it's impressive to see a lot of the advances in distribution automation and the benefits it's providing. CenterPoint has an incredible DMS system with -- they treat communications with almost as much importance as their normal data system. It's a time of great change, but as the Secretary has pointed out the issue around cyber security continues to be a growing issue that we face. What I'd like to do today, my understanding is this group is looking

for where you can advise and provide guidance to DOE in terms of next steps and things that DOE should be doing on their agenda. So what I'd like to do is just quickly highlight a couple items I was given, I think about, 20, 25 minutes. And I'd like to speak from, not PNNL perspective, but from the lab system itself, the laboratories, there are 13 laboratories working together in support of DOE's grid modernization initiative. And I'll share with you, sort of, from our perspective what we see going on in industry, what's working well, where they seem to be lagging, some remaining opportunities. I'll give just a very brief broad brush in terms of the DOE activities. I see that Hank Kenchington is here, I know later in the agenda you're going to get a deeper dive in terms of some the activities going on within the Office of Electricity. But then I'll talk a little bit about some of the views that the laboratories have put together for the new Administration this spring in terms of some near terms opportunities to rapidly close some gaps, not just things that

the labs could do but just from a standpoint of what could the nation do to close some gaps related to cyber. I'll talk a little bit about some of emerging or fundamental science and engineering activities that we see emerging that can be part of the tool kit for touching on cyber resilience issues going into the future. And then I will suggest-- I'll close with some key questions because I think this Committee is-- has a very compelling opportunity, you have an opportunity to help advise the Department in terms of what's most important to do next? In a journey of this Nantucket sleigh ride that's very important to the nation and I urge you to please let us know where we can help out along the way.

So to some degree I realize most of you know a lot of these facts but the system is getting increasingly dependent upon additional components of communication that's began to really accelerate as we kind of got out of the deregulation uncertainty of the mid-90's. So late 90's and early two thousands national investment,

in order billions a year have really began to increase in terms of modernizing the system. The Internet economy has not slowed down, I don't think it's going to slow down, I don't anybody in NERC or anywhere else thinks the digital revolution's going to disappear. GE Digital Energy estimated we have about two billion at the grid edge today, likely to grow to 20 billion devices by 2025. I think one of the most compelling issues is not the number of devices at the grid edge but the fact that so many of those are emerging on the customer side of the meter; so beyond the direct control of the utilities. And so that's really changing the game in terms of the system, how it operates, how it responds, and makes it more complex for operators to be able to predict and know that the system is going to respond in a reliable, predictable fashion.

The US grid is under constant attack. There are limitations about what we can talk about that in terms of an open meeting such as this but those attacks are increasing. They do include

foreign states. The energy sector in general takes the largest fraction of those attacks if you look at it across different sectors of the industry. So the energy sector is a prime target for those attacks; so it is reality that we have to deal with. And I believe that industry has responded significantly and strongly, but not completely. There are still opportunities and issues and risks that we need to face and I'll try to highlight some of those from our perspective based upon things that we've seen. So one question people ask is well so why DOE? We're in the time of Administration change and so they'll be a lot of new folks arriving in Washington, D.C asking the questions so what's DOE's role etcetera? Congress tried to sharpen the clarity in terms of what DOE's role is. Fundamentally, when DHS was formed they seated back to DOE the subsector accountability for electricity and oil and natural gas subsectors. So DOE has been working with them for more than a decade on cyber security issues for those two sectors. The Fast Act gave more

clear authority to the Secretary in terms of what to do in times of cyber attack etcetera. So the accountability very much rests with Hank and a lot of the other folks at OE in terms of response to events that occur.

The National Laboratories bring to the table a unique asset in terms of being involved with the classified side of DOE's world. The DOE labs had a large amount of classified work that goes on in support of the intelligence community related to nuclear nonproliferation etcetera. So that's a fundamental capability asset that the federal government has in terms of the laboratory staff who understand and have clearances to work on classified issues that sort of bring the high side issues down to bare to engage with in support of the energy industry as they deal with cyber security. DOE is also a steward for fundamental science United States. I believe my facts are correct; they are the second largest provider of fundamental science funding behind National Institutes of Health, is that correct, Hank? I

believe the NIH is the primary federal investment in science, but DOE has a very large investment in science fundamental computation, mathematics, and environmental material sciences etcetera. So the DOE is a steward for fundamental science and where fundamental science can inform the journey to provide solutions to cyber resilience issues, DOE has a fundamental role. So I just tried to kind of clarify what does DOE bring to the table?

From a national perspective, the power system -- we're blessed with over 3,300 utilities in 50 states and 51 regulatory jurisdictions.

(inaudible) has been dealing with this for his entire career. As part of the challenge we have, an awful lot of good work in terms of enhancing cyber resilience but there's an awful lot of incomplete implementation; just fundamental best practices. It's not all science and technology, a lot of it is just blocking and tackling and

good hygiene. And there are a lot of utilities out there who aren't able to step up to meet that bar just because of their staffing and or resource constraints. There are limitations in terms of access to near real time situation awareness particularly in terms of cyber threat. Dramatic progress has been made there and I'll talk that about that a little bit later. But still today we have a pretty small fraction of US utilities who are -- who have access and are aware of what's going on in terms of situational awareness tied to cyber real time issues.

Dramatic growth in use of digital systems and public Internet, and again, I don't think that's going away. And there are profound benefits to the power system and being able to leverage a digital modern grid in terms of

performance and reliability and economic throughput etcetera. And so I think we dare not try to stuff that genie back in the bottle. The question is how do we embrace that, get the full value out of that digital opportunity but do it in a way that gives us the cyber resilience and robustness that we need? And bottom line is, there is increased sophistication in terms of the threat after us both foreign and domestic.

So let's talk a little bit about -- just briefly about the innovation, where does it come from? The utilities are working very hard and I would argue, I mentioned before we have 3,300 utilities, that the middle third are the mid-sized utilities; they are pretty limited in staffs and in resources. I think a majority of the activity going on is more in the larger third of the utilities in the country; and they're doing an awful lot working with NERC on new standards, working to secure their communications and IT business systems. The majority of their emphasis in the on IT side of the equation; has been

historically. There is good collaboration between the executives across APPA, NRECA, and EEI, and the Energy Subsector Coordinating Council; I got ESCC correct. And so there's been an awful lot of progress in the industry working with NERC and the SCC and DOE to advance the ball down the field substantially. The vendors are doing an awful lot. Much of it I would quantify vendors and utilities, all of us, for the last decade, more in Ketchum patch and trying to identify vulnerabilities and close those vulnerabilities. A lot of their solutions are proprietary and some cases that creates a bit of a barrier for some of the utility innovation activity, but an awful large group of vendors who are very active in this space and doing an awful lot of good things to support the industry. The laboratories tend to be more on the fundamental side of the activities. A number of laboratories, I just picked five or six here, my guess is all laboratories work in cyber to some degree. Sandia does an awful lot of work of encryption. Oakridge, Tom King is here, he also

works with me on the Good Modernization Activity. Tom wave your hand; he's a good southern boy, he's safe. They work in alternative communications and other activities. Idaho works in control systems and wireless communications protection. We do a good bit of work at the laboratory in terms of information sharing and technologies on the OT side. Los Alamos is working in quantum key encryption. Broad range of activities that the different lattices bring together and we coordinate and collaborate in large extent on a number of these activities. And then there's the universities. I think, just like the laboratories, a lot -- I'm sure every university is working in cyber these days, but there are some large structured groups that DOE Office of Electricity, actually -- Hank's organization, funds CREDC, Dave Nicol's organization up in Illinois. The Secure Evolvable Energy Delivery Services (SEEDS) Group that's led by the University of Arkansas. A number of small bilateral and multi groups,

PCERC is a long, over 20 years now, group of utilities that have worked together on a number of activities. So there's a broad base of innovation, the challenge is how do you harness all this in some key strategic directions, how do you set priorities, how do you just get the information forward? The Good Modernization Activity that Tom and I work with we had our first peer review this fall, or this last April, and a number of people said this is just unbelievable, you need to get the word out, I mean, it's really hard to keep track of all the things that are going on and find systematic ways of delivering them to practice in the industry.

So now I'm going to paint just a very brief brush in terms of OE activity -- or excuse me -- Department of Energy activities. Office of

Electricity leads this journey. Their activities are the tip of the spear but there are other activities within DOE and I wanted to share this with you because I think it should be part of your considerations in terms of what tools, what levers does DOE have that they can push or pull to help support this overall journey going forward? So the Office of Electricity has the cyber security for energy delivery systems program. It's been ongoing now, I think, for over a decade and they just recently upgraded a Multi-Year Program Plan, they had some awards that were announced earlier, I think, Tuesday morning of this week. Number of awards and there were people in this room and utilities that are participating in those activities and Hank is the expert on that, I think you'll hear more about that in Multi-Year Program Plan later in the morning. In addition the Office of Electricity has an Advanced Grid Modeling Program that about two or three years ago sat down and ask the labs and ERCOT to help frame a more compelling tool to look at, assess the risks of

cascading outages for planning as NERC tightened down their standards for their planning consideration for preventing cascading outages. They asked for a more compelling tool; the old tool was pretty much a static tool. It had no accommodation for the underlying protection systems etcetera. So it gave incomplete answers and so we developed a hybrid tool working with ERCOT and their vendor to put in place something that looked -- that captured system dynamics. It leveraged high performance computing to handle much larger, much more complex scenarios for cascading an outage. It included the underlying protections systems and that is now -- it performed well that ERCOT is implementing it in their operations and we're working with the GE PSLF community now to help bring it to that community as well. And the target is for the nation to have a much more effective ability to protect, predict, and plan and design around a risk of cascading outages going in to the future. And I'll make one point here, a fundamental point,

I think there's risk if we overemphasize fixing cyber because the power system faces a broad range of risks and much of the protection response and operation control and other things to deal with cyber are the same tools that would use to deal with other risks. So while cyber is incredibly important, I believe that we need to take a systems approach looking at all hazards, draw from that those cyber pieces that are critical -- when that's the key driver -- but I think we run a risk if we focus only on cyber, we'll end up creating suboptimal solutions that we'll regret downstream.

So moving on then, RPE, the Advanced Research Project Agency, they actually have a good bit of work in distributing controls that ties into how do you let the system down more easily and recover it more quickly and perhaps protect distributed islands more affectively if there are larger incidents that occur out in the system? And then they are setting up data repositories and modeling repositories because the big barriers for innovators like Blod and Kasinovich and his

graduate students is getting access to good utility data. And so NRECA and others are working with RPE to help establish data repositories that the entire innovation community can access to design either better cyber tools or better distributor market tools or other things. The Office of Science is investing substantially in mathematics centers where they're developing new algorithms to help look at Advanced Control Theory, more distributed Lameter Control Theory which is where this natural trend of the emergence of distributor and energy resources and digital vices on the customer side of the meter etcetera; what sort of control theory do we need to help us adapt and to ensure that those devices will respond in ways that predictable and commentary to bulk system reliability? They're also launching a new program, an Exo-scale Computing. Exo- scale just means billions of billions of floating point operations per second, that's roughly a thousand times, a thousand improvement over current computational capability. The machines don't exist

yet. DOE is in the process of building those machines, they're just standing up programs now to develop utilization of those new exo-scale computational resources and one of their new projects is a grid-oriented product, basically looking at how to capture, in planning, full system dynamics, the full uncertainty about weather, and the full uncertainty about complex demand response and other activities in a 20 year planning horizon to help design more resilient, more robust grids. So that is an early DOE effort in terms of engaging the emerging exo-scale capability for grid applications. One of I think the benefits of the grid modernization effort over the last two years has helped break down some of the barriers inside DOE and we've actually seen a lot of uptake by Energy Efficiency and Renewables Offices who own the energy devices on the customer side of the meter to start paying more attention to cyber security and realizing that they're part of this overall journey.

And then lastly, the office of the Chief

Information Officer (CIO) and DOE, they have a big role in terms of cyber security inside DOE based upon the DOE complex which includes production facilities for weapons grade materials. DOE manages the nuclear weapons stockpile. So DOE has a very large production complex that they have to manage and ensure the cyber security of as well. So I offer this to you because as a -- there are a number of buttons and levers within DOE that can contribute to the overall cyber Nantucket sleigh ride. DOE also works in outreach activities in terms of emergency response that's partly why you don't see many of them here today. A lot of them are dealing with emergency response in the Southeast. DOE was involved in early days of Cyber Risk Information Sharing Program. It actually came from a program that DOE used for the DOE complex. They tried it with a small number of utilities, they then encouraged NERC to take point and the Information Sharing and Analysis Center (ISAC) now drives the crisps of the Cyber Risk Information Sharing Program. Its membership now covers 75

percent of the electricity that's generated in the United States, but it's a very small fraction of the utilities in the United States so it's making good progress but there's more progress to be made there. DOE supports cyber exercises like grid x and working in conjunction with DHS and others. They also developed some of the early maturity models and vulnerability assessments, I think, TVA was the first vulnerability assessment DOE supported back in 1998 or something like that. They usually try and develop the tool and move it out to industry and now NERC and others are driving some of the maturity model activities going on; so a broad amount of engagement within industry on the operation response side as well as the research side. So I just tried to paint for you a number of attributes within DOE that contribute to the DOE agenda, a number of types of roles that DOE can provide and support going forward.

The last thing I'll mention is the Grid Modernization Initiative. I know this has been

briefed to the Committee before but we do have some new phases, Mladen, I'm going to make you sit through this and there will be test at the end of it so -- In 2014 the Department stood up a Grid Modernization Initiative in response to the Quadrennial Energy Review that Dave Meyer and others spend a lot of time working on and they launched -- they asked the laboratories to support in more coordinated, collaborative fashion. We still have to compete; there is the fundamental science philosophy of competition of new ideas. But we basically put together working with DOE program offices a multi-year program plan that had an integrative strategy across DOE. There was a lab call about two year ago, about $220 million, two-thirds of which was competitively sourced, one-third of which was asked-- was done collaboratively with this group of 13 laboratories that Tom and I work with. We just had the peer review on that. And within that group, so its $220 million is awarded initially plus then there's a recent award of about 25 or 30 for resilient

distribution systems. There are several key activities that I think contribute: one is the foundational effort in grid metrics. We're trying to update the set metrics that DOE and Congress know this would use to help evaluate the progress of the nation as it moves forward in grid modernization at large. Some of them are the old tried and true affordability and reliability, which we all know and love so well. But then we're also looking at new metrics including resilience, which is you heard from The Academy, there is still no complete convergence in terms of the definition let alone the metrics you use to figure out resilience. But also flexibility, you know, the emergence of the need for grid flexibility to deal with the increased stochastic behavior of the system, to increase the amount of system dynamics throughout the system including the East which used to say, we don't need no sticking phasors because we're heavily networks, well even their getting dynamics in the system now that they're trying to find more effective ways of dealing

with. So, new metrics and also new valuation tools are being crafted to help figure out so how much resilience can we afford or how much is worth paying for? I think back to Sandy when a utility brought to commission in New England a $6 billion opportunity and they said well how much better than that is $4 billion and they really couldn't answer that question. I mean this is hard; it's hard to do that kind of thing. So that's why evaluation is just as important as the science and technology because if you can't answer the evaluation question then your science and technology won't get into the marketplace. Grid architecture, I think is important because this is such a complex problem, it gives us a systematic way of looking at what's going to change and the relationship between key systems inside the grid family but also outside, like communications and fuel supply and other things. It illuminates where we're getting increased grid risk with the new systems and the trend toward the digital systems. It illuminates what alternate approaches

we might have for closing those risks and it also would show where some emerging market concepts like blockchain and other things. They might be good at certain things but they might be creating unintended consequences or problems elsewhere in the emerging system. So we view this as an opportunity to systematically look at change and it doesn't say what you should do about it, it helps you understand what is changing so that we can make better decisions locally, regionally, and at the interconnection level in terms of what the path forward is. Tom King, his group is working on sensing the measurement absorbability. We ask the question to a lot of them, so with all this great new additional technology how much -- what would full system absorbability mean in the year 2025? How much of absorbability do we need, do we want? Do we have the capacity to take advantage of it, what are the road maps in terms of getting there, what price points do we need on censors to be able to afford, say, time synchronization measurement down in distribution systems they discussed

yesterday? So that Tom can sell it to his management at AEP. And what data analytics do we need to try to keep some of the utilities like electric power board and others from being just totally inundating with all the data coming off the new census sweep? So this is a fundamental part of the defense that we'll likely to want to put in place to deal with issues like cyber risk and I mentioned there was a resilient distribution lab call just the other day that was just announced.

So let me switch, I've talked a little bit about the laboratory view of what are the challenges, and sort of the asymmetric response across 3,300 utilities. I've talked about the number of different colors of buttons and levers that DOE has pushed to help support this activity. And we framed some ideas that we thought the Secretary could benefit from in terms of what are some near terms things that could be done with DOE to help support the national agenda? These are not things that the laboratories would have to do. In

fact, the first one is really not a national laboratory deal but we see enough of this issue when we're out working in the markets place that we thought was important to raise. Suggestions were to rapidly prevent the cyber best practice, just basic hygiene in these vulnerable midsized utilities. The smallest third, they had such a small amount of digital technology, they still pretty much got folks waking up early in the morning and going out and re-throwing the closer; not much risk there. The bigger third of utilizes are working really hard with NERC and they had the engineering staffs and the resources and the right commissions and all to help them implement all these practices. The middle third, a lot of them struggle, some of them are doing a fantastic job but some of them struggle they don't have the capacity to deal with a maturity model self-assessment or other things. Dramatically improve near-term, real time cyber situational awareness information sharing that makes the current best practice cheaper, faster, more

available to smaller midsized utilities; I think we can do substantial there in two years. Secure the electric power system infrastructure, lifecycle integrity, and I believe that Fred Seen and others have worked on this. There is not a lot of standardized approach to how we deal with the acquisition, the maintenance, and the removal of digital devices in the system and we think there's a lot of opportunity to help improve that process and the testing and certification of critical components and other things very quickly and we think we can dramatically raise our cyber resilience; then lastly, of the longer-term issue of core ongoing fundamental R and D activity at DOE. So now it comes I think we dramatically close the gap on awareness of cyber resilience by the middle third of the utilities in two years with a concerted effort. I think we can dramatically improve the cyber risk information sharing products to make it more affordable and get the number of utilities increased their substantially. I think in two years we could partner with

industry and others to help dramatically the protection on cyber -- excuse me -- on the supply chain in terms of vulnerabilities and supply chain because we are spending billions of dollars a year in modernizing and we ought to do our best job possible to close the vulnerabilities in that new equipment we're installing as we move forward; and then fundamental research. I talked about these midsize utilities on thinking the range of 5,000 to 50,000 customers, the picture there is Missoula, Montana and we've raised them because the Northwest Public Power Association (NWPPA) that they work with reflected -- you know they received the maturity model in the mail and they didn't really have anyone on staff who could really understand what the hell to do with the maturity model and their self-assessment and to pay for a consultant it's 25 or 30,000 bucks and that's pretty much one to one and half FTE's for their staff and that's a micro cause in what all these small midsize utilities face in terms of trying to close the risk. Now I would argue that

the Missoula Co-op is not a key risk point on cascading failure in the Western Interconnection but there are a lot of other areas and issues that are important from political and local issues in terms of if Russian malware shows up on their systems and other things, there are lots of other consequences that we have to deal with in the world today. So I think there are opportunities, I know the DOE is working with AQPE and NRCA Idol program to kind of test the scale of customers but I think we could dramatically try to close that gap in a pretty short period of time.

Supply chain I've already talked about and it's really a lot of utilities in the smart grid investment grand efforts that we led, what was that, 6 or 8 years ago? One of the big positive lessons learned from the utilities was just having awareness and access to acquisition linguist and other things where they could actually deal with this issue of supply chain certification components and other things. A lot of the utilities have never really been exposed to

that so that was big lessoned learned from that activity. But it goes through maintenance and the upgrades and firmware and everything else and then retirement, lots of things, passwords and other things configuration profiles get left on devices that are sent out to the dump and they don't quite make it all the way to the dump. So a lot of issues there in terms of supply chain. So now I'm going to switch to the geeky side of things and this is a bit of an eye chart but I just tried to put up a potpourri of some of the emerging, more fundamental research that I think has a strong connection to where this cyber resilience puck needs to be 5 years from now, 5 and 10 years from now. So again I'm thinking more in terms of longer term, more fundamental DOE activities. Ninety percent of the activity to this point has been on the IT side of the equation, increasing attention being paid to the control systems side of the equation. It's a very different environment; it's a much quieter environment. Different types of censors, NERC actually requires censors to monitor

the data flow within the OT environment. So it's less of new-censored deal here and more of a new analytics opportunity here to help make the control systems that haven't been compromised. Second point, having just an IT situation awareness, an OT situation awareness we think is kind of a fools mission, you really need to have an integrative situation awareness across both of those systems that's and endpoint we think we need to get to in the next 5 or 10 years. Advanced math and algorithms for distributor control and adaptive control. Adaptive control will basically say you had real time tools that enable you to make more precise control and protections decisions than what we have today where often time systems are seasonally rated or they have very stiff reactions in terms of protection of the system so new control theory I think is an important opportunity moving forward that DOE Office of Science has a strong opportunity to influence. Modeling and simulation of extraordinarily large data sets and I mean even

beyond what we're even looking at in terms of interconnection scale phasor measurement unit. If you start putting time sequence devices down in the distribution system and getting more coordination across distribution automation etcetera, we will continue to see an explosion of data and so there's a need for new classes of algorithms to handle these incredibly large data sets. Some of which have extremely high velocity and require very low latency constraints in the data sets so it's a very different world to curate some of these data sets than maybe what some of the commercial vendors might do for social media activities and others things that utility world has a little different requirements. Applications of deep learning to grid data steps and automated machine-to-machine tools. Machine to machine exchange is a priority for the ESCC, I know. But part of that relies upon new tools where you can actually do that in a trusted a confident fashion. Supply chain risk characterization, we really don't have a handle in terms of how much risk do

we incur from the supply chain vulnerabilities we have nor do we know what metrics we would use to measure of when do we have enough protection on the supply chain side? Novel System Authentication and management methods, looking at new encryptions, use of fontal computing and other activities. Alternative communication networks, how do we take advantage of either dedicated networks or underutilized fiber networks and other things that are within utility ownership? And then new fundamental grid elements that we might add to help plan a new system. I mentioned flexibility early in some of the architecture is pointing to the combination of energy storage who's price points are dropping substantially with advanced distributed control theory, plus smart inverters to make them a more fundamental element for grid reliability managements not just for peak shading and load shading as some of the early opportunities the utilities are looking at now to make it more of a fundamental control and management within the power the system. So these

are -- this is a laundry, kind of a laundry list of the emerging fundamental research topics. Machine learning, someone argued there's a certain amount of circuit lubrication going on with an ocean around machine learning. What's changed from the old journey we had in the early days of artificial intelligence is computations advance where we can now overcome some of the limitations we had with AI 20 years ago. So there are some very profound positive outcomes emerging in machine learning but it's a very cluttered and broad world, I'm sure Mladen and others can share insights on this along the way but we feel that there is some profound opportunity particularly in the detecting anomalies in incredibly large and incredibly high velocity data sets. If you're looking for anomalies where there might be an apparent intrusion on control systems or other things and how do you think that to the special protection schemes in the East or other things and look for are we covered or are we not covered? We think there's some opportunity in terms of machine

learning to actually open up whole new ways of protection particularly on the control or OT side of activities.

So let me close. I tried to think of some key questions that I would suggest to you, and one of those starts with, the seeds came from the National Academy Project that John and Granger and a number of folks participated on, and much of their conversation looked at the issue of well who pays for resilience and who gets paid for providing resilience? It's really not part of the normal value stream within utility infrastructure. Not many people are making money off of that stuff. It's more of a nuisance, a compliance requirement, something they have to do. It's really falls, to a large extent, in that public goods realm. And, Hank I might be wrong, but my sense if you total up OE's budget on cyber plus EERA's putting in a little bit, and the Office of CIO and all, it's probably under a 100 million, I would guess, is that a pretty safe bet? But this is a public good that spans across the nation, how

much of this cyber resilience and resilience to all hazards falls in this public good domain? That's an important thing for the community to think about because it gets down to, well who should pay for how much of some of these new innovations and other things? And I think that this is an instance where there is a very strong public goods dimension to this issue of trying to close our gaps, our risk points, in the nation's power system. How do we rapidly ensure good hygiene across the nations power system, how do you incent the right behavior to get that last group of utilities in through the gates and to the point of where they actually know what their cyber resilience position is? How can we continually improve the defenses both on OT and the IT side? What I like this tool wall, and I'm not picking that because of current politics, no matter how good a wall we build on the OT and IT side, somebody will get through. It's absolutely essential that we can continue to build an effective barrier in terms our digital systems on

this utilities systems, but I also think we need in think in parallel to design an inherently resilient system that falls gracefully, protects, recovers, on the assumption that people will get through that wall at various times. So we must continue to improve that wall, it's a bit of an arms race, as soon as you improve that wall then the opposition understands that so we must and we will continue ion that journey, but at the same time we need to be thinking about opportunities through some of the fundamental research for new design paradigms, new protection paradigms, and other things because somebody will get through those walls in the future and that's just part of our reality. So that leads to this issue of how do you design and transition from a regulatory standpoint to an inherently resilient flexible future system? So that's just some key questions I think are worth thinking about in terms of where would we like to guide this puck, not where it's going to be, but where would we like to guide this puck in the future to deliver on these public

goods issues that are so important?

So if I tried to instill that big list of science and technology, I'd settle on high performance computing for real time predictive operations where we can actually predict system dynamics, predict potholes, steer around them, and deal with anomaly intrusion detection in case somebody does get through walls; deep learning for grid analytics, advance grid architectures for all hazards to inform the theory and control and protection and recovery strategy in the future.

And then lastly the valuation tools that would enable the regulators to provide the path forward in terms of investment or the consumer owners, it's not just regulators, regulators and consumer owners, this issue of how you value: how much do we need, how much can we afford, how much do we want? That's got to be part of the equation going forward.

So I would end with, I've tried to paint a system that has phenomenal challenges but we've made incredible progress. We have great promise

from a digital power system future where we get economic productivity, incredibly precise control on operation that's going to help us steer around potholes to get more economic throughput etcetera. We do have risk from the standpoint of cyber attack and I think you guys as a Committee have a most compelling opportunity to try to help advise DOE on this very large complex Nantucket sleigh ride with 3,300 utilities and 51 regulatory bodies, great fundamental science assets, great utility sector, great vendor community, and great opportunities to build a digital production, incredible system that's not only a great grid but enables a great energy and economic system because the grids becoming more tightly coupled. So it's those other systems that are so important to our vitality; but do it in a way that ensures a resilient and robust future. That's a great homework assignment, I'm jealous. Thanks.

MR. NICOL: All right, very good. Well, thanks. It's an honor to be here and share my thoughts. Something that I often do when I follow

a speaker is make a joke referring to Monty Python saying, and now for something completely different except I can't say that. What may happen after I give my presentation, you say there's an echo in here, because a lot of the points that I'm making, Carl has made more eloquently than you will find from me but I think we're hitting some of the same things. With respect to the way one says the name on the Professorship, it's appropriate, it's like voltage except is Woeltge. So the context, why is it that I was asked to be here? So I'm the Director of Information Trust Institute at the University of Illinois where the focal point for large-scale research and development efforts at the University of Illinois in areas related to things like cyber security. In particular, we have been working since 2004 on issues related to security in the power grid starting with a National Science Foundation (NSF) center called the Trustworthy Cyber Infrastructure for the Power Grid (TCIP), thanks to Hank we were picked up at the end of that center by DOE with a new center

called TCIPG which ran five years and now we, along with the SEEDS program, or the next inversion of that called CREDC which is somewhat expanded from TCIP and TCIPG in so far as we're looking at resiliency as well as security in energy delivery systems which include power and gas as well as power. In addition over the years, we've been partnering with different industries and labs responding to the DOE's various calls. And so I've been involved with companies doing some research that has led to development and deployment of products that are in the field and that's something that we really like to do and that's something that DOE likes to see us do and that's one of the things that really drives the problems that we work on, is how can we have impact, impact measured in terms of having the results of what we do be actually used in the field.

So presently CREDC, it's a consortium, that's one of the C's stands for, of a dozen universities and national labs which includes PNNL

and we're working on roughly 30 projects right now. We organize those projects in the following areas, just to kind of give you a sense, I'm not going to talk just about CREDC, but to give you the context of where it is that we're coming from and the things that we're already doing. So in the area of cyber protection technology, this is cyber stuff that we use to protect the OT side of the systems and so things like lightweight authentication, for example, would be one of those things what kind of security we bring, or reliable communications in context where you don't have reliable communications, things of that type. In the cyber monitoring metrics and evaluation domain, you know -- so I got into cyber security by historical accident, of interest of only to me so I won't go into it, but in 1999 and roughly in that time frame there was a list of hard problems, cyber security hard problems, that were put out and on that list was metrics. How to do you measure, what do you measure that says something about security? Well you know what, they're

putting out hard problems and metrics is still on there. Fortunately on the OT side of power systems there's enough control and structure and deterministic behavior that you have a shot at measuring things and making inferences from those. So part of what we're doing there has to do with measuring things but doing so in a way that doesn't disturb the system. Right? These are real time systems, they're legacy systems, you can't just walk in and put in security stuff and not expect to have some kind of impact on that and so you need to minimize the impact that that actually has. Another area is in risk assessment of EDS technology and systems and this gets at something we've been talking about is there's this balancing act that's going on, is you have these new technologies that are coming up, they provide measureable benefits in terms of productivity, increased capacity for the system and so on and yet they increase the risk to the system and so how do you get your arms around that. That's not a solved problem, that turns out to be one of the

things that I think we need to continue to focus some effort on.

I have an area on data analytics. So the challenge here and Carl made the point is tremendous amount of data available, so the challenge is how do you turn data into information, information into knowledge, and knowledge into action? Because at the end of the day, you know, this is a tremendous amount of data and somebody has to make a decision sometimes and what do you do with this? And frankly, you know, it's an operator or an operator's manager, an engineer, and they have to make the decision right now. And so how do you distill all that stuff into suggestions, an understanding of what's happening and provide an answer to what it is that you need to do right now? How do we architect systems so that they are more resilient to cyber disruptions and so there's a lot of things that you can't tack on to a system after it's already been designed: performance is one of those things, security's one of those things. You can try and you can improve

it somewhat but what are the foundational principles so as you develop these systems you have these properties that you know give you the resilience that you need and so that's a very important -- what tools and technologies to use and so we are interested in software define networking, I'll say something about that later, but that's a tool that one can use in this particular space. Disruptive technologies, they emerge on the horizon. They have impact. It's interesting when TCIP first started we had meetings with computer scientists, computer engineers, power engineers on the academic side, and then we had utilities and there was a fair amount of talking past each other because, you know, the academics were coming in and they had these fancy shmancy, you know, dynamic Bayesian base decision making frameworks and the utility guys said, huh and other utility guys said we're not connected to the grid so we're connected to the network, we haven't got any problems at which point somebody asks, and how do people make a

connection to do remote maintenance? They say well they dial in, say connection dial in -- well, any way so the point is, it came together at a point. The academics, they wanted to go off in Lala Land, went back to Lala Land, the one's that wanted to work on real problems stayed and listened. So the utility people actually learned. But one of the things that was interesting at that time, as it comes to disruptive technologies, is people said, you know, wireless technology was taking off at the time and people said, there's no way we're having wireless internet well, okay that was then and this is now and wireless is a tool to use in this context. So this happens, you know, these technologies emerge and you can point at them and say, we'll never use that, that's too dangerous, but it happens. And so there are other ones like the cloud for example, I mean the cloud has lots and lots of economic advantages but it changes the risk profile so how do you understand that another disruptive technology you can imagine is the proliferation of electric cars because there's all

sorts of things that might happen when you have lots and lots of electric cars, you can have a parking lot full of batteries that might be used for some kind of support and control of the grid, for example. While there's all kinds of things, you know, that's going to be enabled in a cyber sort of way but you have to be concerned with privacy, you have to be concerned with billing, you have to be concerned mobility, you have to be concerned with all kinds of things. So the point is, this is why it's fun to be an academic; sometimes you get to dream about this stuff. You say, what would happen or what's going to happen as these things, these trends that you see happening emerge and have impact on the things that are really important to us. And finally validation and verification, you know that's the challenge, of doing the right thing and doing the thing right. Sort of the difference between the two, that's a big effort that we have, is as we develop these technologies that we intend to have be used and aren't being used, we need to

verification and validation (V & V) on them to increase our knowledge of what they're capabilities are and also increase confidence that others may have in those. So again, the emphasis at CREDC is the expectation is that we move this research that we're doing into practice. If we don't see a path for the research that's going on to something that will sooner or later, preferably sooner, lead to something that's something in practice, then it's not in the portfolio.

One other program that ITI supports, I want to mention because it has relevance here is the DARPA Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program. RADICS is about developing technology that will help restore a large chunk of the grid, think of the Western Interconnect, in seven days after a cyber event has disabled it. And so there are things that are called DARPA hard problems, I call this a DARPA impossible problem. It's setting the goal and to aim at. The piece of this that we have is the test bed and framework for evaluating the

technologies that are being developed by other performers. And so the test bed that we have is going to be playing a role in grid x, I think there's opportunities and resources there for other kinds of exercises based things and we can thank you friends at DARPA for investing a lot to help us improve the test bed facilities that we had so that we can do things like model the western interconnect at certain levels that are appropriate for detecting when there's something miss, modeling something on the scale of a large utility so that allows performers to go in with their cyber hazmat suites and go and find the bad stuff and get it out and restore the grid. So that's sort of what it is that we're doing the rest of this is where we get into the echo chamber and that's the areas where I think that there attention is needed.

So Carl mentioned right at the end of how the challenges that we face here really can be viewed as a public good. Whose problem is it to make the grid resilient? And that's a hard

problem, it is a public good and it requires investment by the government when viewed that way but that's in the future, I mean there are some really good things that are happening and more good things will happen in the future but, you know, to have impact right now we have to be looking at way that incentivize business or utilities to choose to invest in these new security technologies. Which means that you have to be able to speak the language that the decision makers understand, you have to be able to translate this into dollars in one way or the other. Now it could be risk; you could say, well you know if we don't invest in this technology then this really bad thing could happen and it will make so many dollars to disappear from our income and that's all fine. The classical formulation of risk is probably times cost so what's the probability of this thing happening times the cost of this happening, so okay you can nod you heads up and down, you say, wait a minute, what's the probably of an event happening?

That's really hard to quantify here. And so it's hard to quantify, and furthermore there's psychological studies that show that people don't act rationally in the sense of mathematical sense of rational in choosing the outcome with the best expected utility that they are inclined to ignore or discount rare event high consequence source of events. And so we're faced the problem that selling fire insurance is a hard sell because it's hard to quantify that into actual dollars. So there is a finesse or there is a space where you can address some of these things and those are technologies that advance security, while adding other kinds of value that are quantifiable that can be argued to make sense and improve the business on a day to day basis. And I'll give you two example of that; some has to do with monitoring and analysis technologies, you know, you're watching things that are going on, you can say well we're watching thing to go on to find those rare events when bad things happen, but you're also learning a tremendous amount of the

way the system is working and when you understand the way the system is working you can make business decisions about it, reorganize, and optimize your system because you have a better understanding of what's going on. And so I think there's areas in data analytics where we can make this argument. There's other technologies that will lower maintenance cost and I promised I'd get back to software defined networking and this is a great example of it so we worked with Schweitzer Electric on a project funded by DOE to develop software defined networking controller specifically for use in the power grid. Now the interesting thing there is that the use, the original origins of software defined networking were in the wild, wild west literally of data centers in California and all kinds of crazy things going all the time and so software defined networking was a way of trying to manage all of that in very dynamic way. [Unintelligible] but what this gives us is a uniform way of thinking about our networks and so we can design our

networks to behave a certain way, we can engineer our networks and in engineering our networks we have better understanding of what it is that they're doing and we lower our maintenance cost in doing that. So there's a win-win there because with software defined networking there are a number of things that you can do with that technology when it's in place to improve security. Another area I think needs attention, Carl pointed at this and this is in information sharing. Lest I give the impression that I think nothing is happening in this space, that's not the case at all. Cybersecurity Risk Information Sharing Program (CRISP) and Cybersecurity for the Operational Technology Environment (CYOTE) are a couple of programs that DOE's doing right now recognizing the need and moving forward, but the fact remains and Carl eluded to it, while their programs are there, the participation is small in terms of numbers and so the questions really are what are the incentives for entities to participate in this, what are the vehicles for

sharing? Having the data repository be at the government is probably a bad idea, I am from the government, I'm here to help, you know how well that works. So there are ISACs that help, but independent third parties where the information would be shared and distributed seem to make a lot of sense but one of the reasons why people don't involve themselves in information sharing is that the risk of letting loose something that they preferred not be let loose. There are some very real privacy concerns in involved in this. And some of it might have to do with economic reasons, some it might have to do with well if somebody sees my system is doing this then I might be inferred to be in violation of something or other and I could get in trouble, so there are reason why people don't want to share information. There are technologies one can develop that help that by doing anonymization and privacy protection, it's important you do this in ways that you can prove the properties that you've got from the techniques that you apply. Because just a heuristic, I will

do this, I will remove personally identifiable information from this is not enough because breaking privacy is a matter of triangulation. You have some anonymized data it has enough things in there so you can correlate with other indicated outside of your space that say because of the things I see and hear the only thing that matches that is this entity out there therefore that's what this entity is and so there's some challenges there and so some research is needed there.

In CREDC we have been focusing a lot on protecting the grid and trying to manage things when the intruder does come in, again that's another point that I want to echo that Carl made, you know I think that you have to assume that the bad one can get inside when you have nation state actors that bad one will get inside and so if we're going to approach it from the point of view of really protecting these critical assets you know you have to A) raise the bar so it's harder to get inside but B) be prepared to deal with the intruder when the intruder is inside. So that

means that if the intruder gets inside the intruder may actually cause some damage to happen and so the challenge then becomes how do you recover quickly from that and that's what the RADICS program is about but I will at least say that I don't see a lot of that happening right now, elsewhere aside from the RADICS program and I think there's some real challenges there but I think there's some promising technologies as well. One of those would be virtualization and so if you imagine having your processes and your network is running industrial control system be virtualized that means that you can wipe them. Say, I think this device here might be compromised, I can bring in a gold standard, I can, you're gone, new gold standard is in there. And so there's possibility there that you could do this quickly. Less clear what you could do about data that you're gathering on the fly that your system is running but again there are some things that you might be able to do that involves starring data so that you can recover it very quickly. But the point that I

wanted to get to is that I think the recovery aspect of cyber intrusions is being underserved and we need to be able to that -- and this is another place to get back to, a place that they made earlier, is that we need to close the gap between expert knowledge or expert technology that's detecting when things are wrong and replacing things when they're wrong. But the people that are doing this, they need to do it now and they haven't got PhD's and so you need to be able to translate this highly technical stuff into actions that can be made by ordinary people right now and that remains a challenge.

Other areas that need attention, and I believe is my last slide, is assessment. Again I want to not suggest that there isn't activity going on, in assessment the IC2M2 program is showing the way there but assessment is our tool to be able to try and reason about some of these tradeoffs so there again, there are emerging technologies, the industrial internet of things, cloud computing, a lot of really good driving

economic reasons to use this stuff and they will improve productivity and they will improve capacity and they increase the attack surface and so there's this trade off, you have to understand what the attack surface is, you have to protect yourself with the knowledge of what that new attack surface is, you have to be able to assess, the question is should I allow someone who's doing maintenance to combine with their iPad and connect to my thing using a wireless connection? Well, the answer's probably no but at least without some kind of protection but the point is, that you need a way to be able to ask and answer those kind of questions and at the end of the day it comes down to dollars. At the end of the day when it comes to decision makers they'll say, what does it cost, what does it cost me if I do this, what does it cost me if I don't do this? How do I reason about this?

And then finally I think that there's work in improved trust and communications in prominence in digital artifacts. I'll just give

you two examples, current example to illustrate the point. So you will remember that of the steps in the STUCKS Net Attack there was a USB key that put into a laptop and there was a piece of software on the USB key that represented itself to the laptop as a driver. And it proved that it was a driver because the software on there was signed and the private key that associated with the signature belonged to a Taiwanese manufacturer. And so the operating system did what operating systems do, they say here's a signed artifact I will do my cryptographic check. Check. It's the driver. It installs it; except it wasn't. It was something else. And the problem there was there was only one check. And so the solution in that particular case is maybe to have some more checks, to raise the bar to make it harder to fool systems when digital artifacts are presented. I'll give another example and that is in the 2015 attack on Ukraine, the way the attackers got from the business side to the operational technology side was through a VPN tunnel that they got by

purloined credentials; stole them, used them, and after that they were good. They were checked once, only once against, you know, one set of checks and never again. And so there are ways one can deal with this and the challenge is how do you do this in a way that doesn't disturb the system, how do you increase the number of checks that you make without slowing everything down, what should you check, how should you check it, what should the (inaudible) be? And so on and so forth. So that's it. I hope you think that maybe there's an echo in here, hitting on a lot of the same points. So I'll pass the talking stick on to the next guy.

MR. GRIECO: Did I do that? Impressive. All right, my name is Anthony Grieco. I'm from Cisco. I appreciate the opportunity to be here amongst this distinguished audience and then the distinguished panel. It's really humbling to look at the depth of knowledge that's brought to bear in the context of the power community that we all

depend on in this room today.

When I look at this conversation and think about it, I'd like to give it a little context. Many of you know Cisco as maybe a networking provider in the context of communication systems that you have today inside of your enterprises. Some of you may have some of our products and services deployed in the context of your power distribution systems as well, but there's a different lens that I want to bring from a Cisco perspective into this conversation and it's really focused around security and IOT.

In particular, when we look at the global conversation that's happening around security and IOT, we are helping our customers globally think about and understand cybersecurity risks as it relates to IOT as they look to digitize their environment. So while you may know us as a communications company, realize that as a part of the recent history of Cisco, we have really expanded what we're in doing in the context of cybersecurity.

But there's a rich history here that I think we are looking for ways and encouraging others think about as it relates to resilience of the infrastructure itself. It's no secret that the internet itself is something that is critical for communications not just for your networks and the environments that you operate, but also many other critical infrastructures around the globe. And for years, we have been building into those routers and switches and the things that facilitate those communications, a series of things that really look to address the fundamental ideas that have been expressed by a number of the other colleagues here today.

How do we talk about resilience and robustness in the face of attacks? And so when we think about this conversation and the context of the power infrastructure, we think there's a lot of similarities that apply to certain areas that we should be looking to explore how we can share information and knowledge about these things.

The first discussion for this topic for

me is a realization that the game has changed. I have the privilege of being at Cisco for 18 years. I am a cybersecurity person. I'm not a power person. I have lived in the cybersecurity world for the past 15 years and the acceleration of importance of cybersecurity over those past 15 years is undeniable. It is the number one conversation that I have with every customer in every vertical around the globe.

I have the privilege of going around and speaking with governments and critical infrastructure providers around the globe, and their number one concern is cybersecurity. So this conversation in the context of the power vertical is something that is really critical for this discussion, but realize that you are not alone, but ultimately, when I look at the power vertical today, one of the critical things that I think is important that you all probably are aware of, but is really important to emphasize in the context of this conversation, from my perspective, the game has changed.

The maturity of adversarial activity over the past five years in this space has accelerated beyond anything that we had seen in the previous decades. And in fact, we see adversarial activity that is really looking forward, something that everyone needs to be aware of. First and foremost we see adversaries attacking not just the individual providers, but also people who are providing services to those providers.

It's not just about an individual target at a, say, a cooperative that is providing power distribution. They're also looking at the ecosystem of people who they may be doing business with as part of delivering those services. So whether it's an HR partner or a finance partner or any of those others, those are avenues that adversaries are considering as a part of their direction.

Second major thing that we are seeing that is illustrated by what happened in Ukraine, but we see it across the board in the

cybersecurity space, there is an immense interest in destruction of service. It is no longer the idea that we're just going to look for adversaries to steal information or otherwise look for intellectual property. The goal in many cases we're seeing is an increased emphasis on just destroying services.

The motivations behind that are many, but ultimately, it's a real outcome that we think about. It's not just about taking information or stealing information. In many cases we're looking at destruction of service.

In every one of these instances we look at adversaries using the latent risk that exists within existing systems. They come in through IT systems. They are exploiting weaknesses that in many cases are well-known and well understood in the IT infrastructure, and using the IT infrastructure footprint as a place to then go and begin to compromise OT and operations systems.

Ultimately, this use of very well-known and very well understood vulnerabilities gets to

some of the points that some of my other panelists have talked about which is there are some good hygiene and basic things that we should be thinking about making sure are happening in the context of the infrastructures that you're operating, that ensure that we are not exposing the low-hanging fruit that would allow adversaries these activities.

In particular, I'll give you a data point that is stunning to me, and it's very telling in the context of this latent risk conversation. We've scanned the internet and looked for Cisco infrastructure devices. No particular knowledge because they're our own devices, but just looking on the internet and looking for them, we've found, you know, 110,000 devices that are routers and switches that are sitting out there that are at the core of infrastructure of somebody's business, potentially yours, that are out there accessible on the internet in a way that we can observe what's going on in them. And 92 percent of them have known

vulnerabilities, 92 percent of them have known vulnerabilities.

On average, there are 26 vulnerabilities across that total population of devices. It's stunning the lack of basic hygiene that we see in the context of our customers today, and a particular, I think it's an important consideration to understand how this organization and group can really look to focus on those basics of better hygiene as a key focus area for this conversation.

The other transition, I mentioned I get to go talk to people all over the world about this topic. One of the key things that is undeniable, and it was mentioned earlier as well, you're not putting this genie back in the bottle. Everything you are doing is going to be communicated to a communications network in order to facilitate the business that you're operating. Whether it's enhancements around digitization to get more sensor data to do analytics on it, whether it's to do predictive maintenance, there's many different

reasons why you are going to go down this path in every aspect of your business.

And ultimately, that transition of digitization is one that is going to disrupt what's happening. I will tell you that when we see the attempt to put the genie back in the bottle, to use that analogy, there is not a single instance where I've seen a company or a customer try to say, no, no, no, we're not going to digitize this. We're not going to bring that sensor data back, where the line of business or the operations people that were getting the benefit out of that enhancement have not found a way around the controls that have been put in place.

So do it because they're digitizing their business because it makes sense. And the same thing's happening in the power space. They're doing it because it makes sense to the business. And so as we look at that trend, there's a really important cultural shift that needs to happen to it that I'll talk a little bit

about in the future.

Finally, this latent risk idea is something that's really critically important. I cannot emphasize enough when we look at everything that's happened in Ukraine, you look at Stuxnet and you're talking about IT compromises that are happening not just in the power industry, but happening across financials and many other verticals where you talk about compromise of systems targeting administrators and looking at them and using their credentials, in many cases, in order to infiltrate the operational side of the network. This is really fundamental operational tactics that in many cases, the damage from or the opportunity to even exploit are preventable with the deployment of the basic hygiene capabilities that we know how to do today.

So looking forward, when I think about recommendations there's really something cultural and fundamental that I think is -- needs to be taken into many industries and as I did research in before coming to this panel, I think it really

is fundamental. There are great number of technology advancements that can be deployed to help the overall cybersecurity posture of the environments that you operate, but I would encourage you to think about a couple of things slightly differently.

You need to think about security as a part of how you are embedding it into your business as an enabler for the growth and profitability of your business. Ultimately, when we look at security, we see it used as a whipping post, something that scares people, something that scares them away, and stops them from doing something. I just told you that you are not going to stop the digitization. You're not going to stop the connectivity. You're not going to stop the deployment of OIT. You're not going to stop the analytics.

And so it's critical that mentally we begin to immediately shift into this idea that security done properly can be the enabler for growth in the context of your businesses. So we

did a study of a 1,000 CIOs and CISOs across a bunch of different verticals including the power vertical. And we asked them how many of them were embarking on major digitization activities and 78, 80 percent of them said they had at least one major transformational activity where they were looking to leverage IOT data and analytics to transform their business.

Yet that same group of people had almost percent, percent of them had stopped one of those major initiatives that were there to transform their business because of cybersecurity concerns. So you see this tension happening, and what we see customers, the most successful customers are the ones that are transforming how they're thinking about cybersecurity as being an enabler, not something to stop the conversation.

And that goes to a second point which is really critical. I'm a technologist by background so it's interesting for me to focus so much on some of these nontechnology activities here, but

and I will tell you I've seen it in spades as I've been involved in the limited amounts within the power industry. Changing the culture around security is going to be critical.

I grew up in cybersecurity. I've been doing cybersecurity for quite some time, and for so many years, we were the special people that were kind of cordoned off in the corner of the room with tinfoil hats on and those are the special cybersecurity people, and nobody really deals with them because they're the ones that have to worry about the cybersecurity.

If you are not finding way to train and educate everyone inside of your organizations to their role in cybersecurity and what it means to be aware of cybersecurity threats, you're doing yourself a disservice. Effectively, it's not that everybody has to be a cybersecurity expert, but everybody needs to have some basic understandings of what their role is in the context of building a more resilient and robust environment.

The other thing that we focus on quite a

bit and I believe you all have a tremendous opportunity to do this within the context of the power grid given the maturity of many of the different risk models that you have is think about how you embed security into all the decision-making that you do. There's not one in here that -- an organization here that can't tell you the impact of a downstream power distribution system that goes 180 degrees out of phase to the overall power grid. But I bet money many of you cannot talk about changes that you're making on the power side or changes you're making on the IT side and what its downstream impacts are going to be from cybersecurity perspective. I think that level of maturity that you've reached in how you manage the grid needs to be thought about bringing a parallel in the context of the cybersecurity and communications infrastructure that supports that grid.

And then finally, I would argue that there really needs to be a rethink of resilience. A couple of my colleagues mentioned this idea,

ultimately, when you think about destruction of service attacks, and you think about destruction of service as a primary goal, recovery is going to be critical, and recovery not just of the power systems, but also the dependent communication systems that support those.

It's not just about getting power back up. You need to also think about how do you go back operationally at the full scale of the communication systems that support that power system. So with that, I'll end there, and look forward to the questions further, and pass it off to my next panelist.

MR. HOUSE: Thank you, Anthony. Hi there, it's good to see you all. Thank you for inviting me. A very impressive panel, I've learned a lot this morning.

It's probably good that I came last because I don't recognize in the work I do a lot what you've heard up till this point. No echo. I find that I live in a quite different world so had I led off it would have been disrupting. Now I

can -- you can take this solid base that you've had which is very informative, and I think I'll be a bit of an aberration to it.

It's good to see you all. I'm glad you're all working in the field of cybersecurity. It needs all the help it can get. I was asked to speak about a couple of things. One was the experience in Connecticut of the regulation of public utilities, how we created a cybersecurity strategy and put it into an action plan. Secondly, based on the success of that plan, how the state itself has created a cybersecurity strategy. Third, what work we do with the federal government. Fourth, fusion centers; how they work, what they do, and then finally, response and recovery.

So a few points on all that and I'm also looking forward to the panel discussion because that will be a lot of fun. My going into cybersecurity is rather simple. My last -- I did, as was pointed out, I've done a bunch of different things in the private sector, national security,

and so forth. My last incarnation in Washington was with the Director of National Intelligence and with the National Geospatial Intelligence Agency. I decided to go back home.

I'm from Connecticut. Went back home 2012, and to be Chairman of the Public Utilities Regulatory Authority, and when I left, colleagues at Department of Energy, especially FERC, but also in the intelligence community kind of pulled me aside and said, look. The United States has a profound vulnerability to cyberattack and most of it is in the states. But the feds don't have anything to do with that and that's a problem.

All the regulation of natural gas, electricity, water that is distributed within the states is under the purview of the states. It's like the insurance industry. The insurance industry is regulated by the 50 states, same with the public utilities. And they pointed out that the regulators of public utilities are overwhelmed. They do gas, water, electricity, telecoms, they're responsible for law,

engineering, finance, mergers and acquisitions, rate cases, and they have 30 or 40 people. A lot of them are former legislators, great people, but they don't have a cybersecurity staff.

And you're saying and on top of all of that, you want me to do what? There were, when I was there, there was about 400 regulators for all the states. I'm sorry, 200. Four of us had security clearances. I had mine because I was coming from the world of intelligence. The other three were retired military.

So the states were not equipped to take this on. They said we've got to have one state get out there and start doing things. If you can do it, that would be terrific because that will point out some of the things to be done. My governor, Governor Dannel Malloy, of Connecticut, I talked to him about that. We used -- in Connecticut we get hurricanes and ice storms. It's been going on ever since the Earth cooled.

We ought to be able to handle them. They're predictable. There will be ice coming in

Connecticut this winter. Hurricanes happen in the United States. We should be able to manage those as utilities and recover from them because it's happened. Ever since I was a kid I can remember hurricanes coming up.

All right. We've never done a cybersecurity attack. It has not happened. So the governor said, yeah, please put together a strategy. I did, and in 2014 issued, all this is available online and I'd be glad to give you guidance as to how to get there, issued a strategy, and I worked with utilities, put it together, sent them copies, said what do you think of this?

It came out. The governor announced it in the presence of the CEOs of the utilities in the general assembly, in the media, and one of those he called for was an action plan to actually take steps to assess and take remedial action on cybersecurity. Now as a utility regulator, most of the times what we do is we have what's called dockets and formal sessions. You come in,

everybody in the room stands up, you simply -- oh, please be seated. They sit down. The lawyers plead. It's all recorded. Motions are made and in our august wisdom we then retreat and render a decision and thus it is and it shall be the law of the land.

Well, I said to him, you know, how do you want to do this because they had resisted. A lot of them said everything's fine. Let me just stop and make a point here. There are a large number of utilities in the United States that have been or are now penetrated by foreign powers, and they could pull the trigger if they wanted to.

Now I think a lot of people don't understand that. They don't accept that. This is not a matter of defending against. The penetration has taken place and the trigger could be pulled if a nation-state decided to do so.

Now we sat down with the utilities and they had put forth a number of the arguments, the error gaps and this and that. And at one point, it was a private meeting. I just slapped the

table and I said this is bullshit. You are telling me things that are not true. Let me tell you four ways you can bridge and error gap, and I want through them. And these guys are looking at me and they didn't have security clearances and a lot of them were -- they were technicians but this was a conversation that had never even taken place before.

And I said how do you want to proceed? The action plan calls for this happening. Do you want us to have a formal docket and we'll lay down the law and tell you what to do or, I said, can we work it out? I said, I would rather work with you and design something that you like and that you're going to accept and make successful, and they agreed. So we had what's called technical meetings.

It looked like the design here. No lawyers, no recordings, no formal motions. We wore suits. It was serious, and we got gas, electricity, water, and telecommunications, and talked about an action plan.

Now three of the four decided to move forward; gas, electricity, and water. Telecoms refused and they refused to this day. The telecommunications, cable and broadband, are not effectively regulated by the federal government nor are they regulated by the states, and they saw cooperation in cybersecurity as the slippery slope toward reregulation. So they said we're not going to play ball on this.

The others did. We came up and very simply we agreed on three things. One, there would be annual reviews of the cybersecurity defense capacity, and improvements of their defense in the state of Connecticut, annual. Secondly, the utility -- and they'd be private meetings. The utilities could bring whomever they wanted. Bring your technology, your finance, anybody you want, any consultants you want, but from the state, because we're talking about the very sensitive defenses of a utility, there would be four people. Two representing the regulatory authority and two emergency managers, that's the

second point.

Third, we said okay, you can pick the standard by which you will be judged. And it turns out there were, because now all the electricity companies own all the gas companies, there are four utilities. Eversource of on-grid Connecticut water and acquiring, each one independently chose the cybersecurity capabilities maturity model known as C2M2.

So we launched this past year. We held those meetings. They started in February. They ended in April. In-depth, and I can say Anthony made a very good point about it's so hard to change culture. I could tell you there's been a remarkable cultural change in those utilities in 2016, 2017 from when I started in 2012.

We met with them. We had very thorough meetings, and by agreement, the report has to be approved by both those four players, and the utilities. I wrote it. Three of the four said yep, it's good, and the fourth has said, let's pretty good. Give us another week. This'll come

out by the end of September. This is, I think, the first time in the United States, I'm told by the media, that a state authority has met with utilities to review in-depth the technical details of a cybersecurity program.

And so when it comes out, if it's of use to any of you, take it. Run with it. Plagiarism is good in this field. The more we learn the less we have to reinvent the wheel. Okay.

The reviews, they made impressive gains, frankly. And it was all done voluntarily rather than a docket and sitting up there and hearing motions and this and that, we sat around the table and said what makes sense? And I got to tell you, that was a breakthrough, and I'm so glad we did it because cooperating with the utilities; the CEOs would come down to the meetings sometimes. The boards of directors knew this was happening and the boards said we want to know what happens in those meetings. So we've caused a significant breakthrough.

Now based on that, the governor of

Connecticut, we got some national media attention for all this sort of stuff and he said what is all this kind of thing? What is going...? I said, Governor, you announced it. You ran it. Yeah, yeah, yeah, but I'm reading the stuff in the paper, and I go to conferences and people say Connecticut's doing great stuff. What is it?

And I reviewed it with him, and he said, well, that's great. I don't want you to stay in as Chairman of the Public Utilities authority anymore. I want you to put a plan together for the whole state of Connecticut. Well, I used to have a staff of 75. I don't have a staff anymore. You know, when I walked in the room everybody stood up. Nobody gives a damn when this chief cybersecurity officer walks in. It's a lonely job but it's an awful lot of fun, I got to tell you.

So we started last October, put a strategy together, and the Governor is really ambitious. He said five areas I want you to cover, state government, municipal government, private business, higher education, and law

enforcement. So we did.

I came down and talked to my old buddies in the intelligence community and defense. And I said when you see Connecticut for private business, what do you see? What are the priorities? And they said three things. The first is what we see in every state, the critical infrastructure of the public utilities. Okay. We're working on that one.

Secondly, the defense industry, you make nuclear-powered submarines, Pratt & Whitney jet aircraft engines, Sikorsky helicopters, things like that. Okay. Third, you do a lot of insurance up there in Connecticut so insurance and the financial services industry.

So we worked with all of them. We came up with a strategy, and the governor announced it on July 10th of 2017. We got some work to do. Simple things, like just as an example, there's a heat map, and you can look at your state and see what the gap is between what business community is asking for in terms of cybersecurity warriors,

people who can come in and help build cybersecurity defenses, and what's being provided. In Virginia just since we're in Virginia, there are 16,000 cybersecurity jobs now going vacant. The total for the United States is 350,000.

Connecticut's a small state, 4,000. But when we looked at the education system, are they being produced? We talked to business. They say we like a two-year degree. Give somebody the technical ability to look for malware, to fix the system, to clean it up, to make it safe, we'll teach them the rest. Coming out of the Connecticut community college system in 2016 there were about 20 graduates.

Throughout the state for the state universities, we also have some small ones like Yale and Wesleyan and Trinity and so forth, but the state university system there were a total of 300 students studying computer sciences, cybersecurity, that sort of stuff. In other words, we're not making it. We're not there. That's what the action plan has to be.

My job now is take that strategy and turn it into an action plan. How are we going to fill that gap? There are few others. An obvious example is how do you investigate a cybercrime? Most states do not have an investigations unit anywhere in the state.

If something happens, you can call the Secret Service or the FBI. Now if it's a bank, and it's a million bucks, the Secret Service and the FBI will be all over it. But if it's the local real estate agent, or a store, or a law firm or something, they like to be told that it's happening, but they can't get involved in a $100,000 heist from a small unit. They just can't.

So we agreed we have to create a cybersecurity investigations unit probably coming out of the state police and it has to be able to provide services to municipal police forces because, you know, a while ago you stopped chasing horse thieves and created a highway patrol. Well, law enforcement does this and they went after

drugs, and they've gone after gangs. Law enforcement constantly adapts to new challenges.

Well, the cybercrime is the fastest growing crime in the world right now, but most states do not have an investigations unit. Now that leads me to the question I was asked to talk about regarding fusion centers. What is a fusion center?

A fusion center basically is a crime investigations unit normally set up with the state police which shares intelligence. And they share intelligence with the feds and with other states. And naturally, because it's police-run they focus on crime. They do a lot of work on things like oh, in New England there's a drug shipment going out of New York. We tapped these two vans. Here's where they're headed. Look out for them. Drug shipments, gang activity, terrorism activity, the kinds of things that you would think of a police force would be useful for. They basically do not get into cybersecurity.

Finally, in Connecticut we have an

outstanding cybersecurity intelligence analyst. We need more. Every state needs more. We do not take the intelligence that is available for cybersecurity violations, break them down to basic police work, and when you do one of the points made is yeah, but how do you do attributions? Some of these crimes come from outside the country.

Three weeks ago there was a cyber hacking activist arrested in Romania for cybercrimes in the United States. My point is this can happen, and at least you got to fight back. You have to know where the crimes are. You have to warn your citizens about what's happening. If you see something happening, tell people. Beware of this. Around April of every year you start getting all these IRS scams that come out, and when you see them in intelligence you should tell people that they're there.

Kansas, Kansas has a great fusion center unlike anything else in the United States. What happened was they were funded by the utilities out

there. So you literally have a wall. When I say literally, there is a wall. It's a structure between the normal fusion center that does the cops and robbers and this other fusion center which has a JWICS wire, that's another acronym, Joint Worldwide Intelligence Communications, from the Pentagon. In other words, they have top-secret stuff coming in there. They have within the utility which pays for this working with the National Guard cleared personnel who can look at where threats are coming.

It's worked. They have both fed the system with threats that they have discovered, and they've also received them and been able to thwart them. Now Kansas, there's only one.

It's controversial. There are those in the federal government right now who say you can't do this. It's wrong. It's structurally improper. You cannot devolve intelligence to the state level to the private sector. That is the purview of intelligence and defense.

Others say if it's helping to make the

country strong, let's go ahead and do it. We in New England have tried to set one up regionally for New England in the state of New Hampshire and we're trying to get -- make a go of that. But there it is. Whether it's going to spread or whether it's going to be snuffed out, it's too soon to tell.

I was asked to speak about overlapping the work of the federal government. There are a couple. One is because our state is the first to have a strategy and an action plan for public utilities, and secondly, because we also did one for the state itself, after the attacks in Europe, the State Department AID went to the National Association of Regulated Utility Companies, NARUC, and said we need a taskforce to help those countries to create strategies and action plans.

The National Labs are outstanding. I think the best one you've got is Andy Bachman who is of the Idaho National Labs, terrific strategist. So they picked Bachman. Connecticut is out in front and I was the guy who both wrote a

strategy and turned it into an action plan. So I got selected.

So I've been working intensely with Ukraine, with Armenia, Georgia, Moldova in -- it was out there -- we were out there in November. We were out there again in April and just a few days ago I met with the cybersecurity team from Ukraine. They have put together, the Black Sea countries have put together good strategies and they're moving forward on all this.

One thing I think is very sobering, you've heard about hygiene. You've heard about best practice and all that, and some of the early penetrations were exactly as the professor described them. They were very harrowing. They were spearfishing attacks, and one of the things they learned in Ukraine was that if you do a targeted spearfishing attack toward not just sending out something broadcast but, you know, going right at it, you, Tom, sitting over there, okay? Tom Weaver, now if I know what church you go to, if I know what university you attended, if

you have children living in certain places, and I send one to you, suppose you had kids in school. And I'd say from, you know, Calvin Public School, you're more apt to click on that.

If I've got something a zoning ordinance in your hometown, you know, I get 120, 150 emails a day, and I got to go through, yes/no, yes/no, yes/no. It's a pain in the neck, and something that's got my daughter's name on it, or something about my school, or my community, or something, I'm far more likely to click through.

What they found in Ukraine was if you do three targeted spearfishing attacks you have a 50/50 chance of getting through, and that's how they got through. They got through and steal the credentials.

What I find far more frightening, and this underscores the basic point, cybersecurity is a matter of offense. The offense is it's an offense paradise. The defenses are very, very restricted. They're very limited and they are unable to provide adequate defense. I mean, that,

you know, the 11-foot ladder is constantly beating the 10-foot wall.

What happened, the third attack in Ukraine which wasn't mentioned, this was in June, and far more frightening than the first two. It was a new form. It was crash over, is what it was, something like that. Sorry?

MR. NICOL: Crash override.

MR. HOUSE: Crash override. You know, it's like the names of the rock and roll bands. Some of these are fantastic, crash override, that's right. And when, I mean, that malware was so powerful and so new it knocked out everything and kind of spilled over and did some communications and others things as well.

The utilities that were affected, and this was frightening, the ones who had cyber hygiene had built up both a culture of defense, software, consultants, and everything else, did all the right things, got wiped out just as quickly as everybody who hadn't. And that's very discouraging because you go around and you say

you've got to do all these things to strengthen yourself. This malware was new and it was so powerful that it wiped them out.

So yes, I work with the State Department AID on Ukraine. I work with the commander of the Cyber National Mission Force. If you think of it in this way, the United States Navy has two jobs. One is to protect the United States from a naval invasion by another country. The other is to protect sea power around the world.

Now quite frankly, you don't -- you're not very worried about a naval invasion in the United States. I mean, that hasn't happened in several years, but that is in their job description. Cybersecurity, if you're head of the Cyber National Mission Force, you also are in charge of not only waging cyberwarfare on behalf of the United States, but also protecting the homeland, and there are attacks on the United States every single day, every single hour.

And so because of the work we've done in Connecticut, I am working with the commander of

the National Mission Force. There's some other states I'm putting also and also the National Guard.

A word about response and recovery, this is -- it goes beyond the norm of what we've had. One of the standard scenarios that people run, and these are just for all over the country, for the northeast, say New Jersey, New York on up, and the six New England states, one of the basic scenarios you run frequently is this. There's a gas pipeline coming out of Philadelphia called the Colonial Pipeline.

Gas is far more vulnerable than electricity. So you knock the pipeline out. Now that means you can no longer refine gasoline, heating oil, and diesel in New Jersey. It does a number on New York City of course once you don't have natural gas coming in.

In New England, 50 percent of the electricity in New England is now generated by natural gas. What would happen if that were to take place; several new things that are not like

the tornado or the hurricane or the ice storm. Number one is there is mass panic usually. People -- what's happened? And the security forces, they are conservative. They're very -- they go by the book and they want to know what's going on before you communicate. With a cyberattack you cannot do that.

You have to communicate immediately and say here's what we know, here's what we don't know. Stay tuned. We'll be giving bulletins every two hours about what's happening, but this is what we know right now. And that's -- there's a gap there between the emergency managers and the natural inclination of the police not to talk about stuff like that.

Secondly, the usual breakdowns will happen without electricity. The cellphones are the first to go because, you know, if you can't charge your cell phone. Food, electricity to hospitals, to, you know, nursing homes, all that kind of stuff. Where does the break come?

Where do you have a fundamental

breakdown in order and a whole new magnitude of talent? Anybody know? Water. After about two weeks you would be shutting down water purification plants throughout New England, and what happens then when they do the gaming of it is that people will migrate. You can put on an extra blanket if it's cold in the winter, or put a fire in a fireplace.

You can open an extra can of soup that you were holding in reserve. In other words, it's not the food. It's not the heat. It's, you know, but if you don't have drinkable water you'll leave. And the prognostications are that if that Gulf pipeline were cut and we're out for more than two weeks, you would have mass migrations.

And my state has -- we have three and a half million people. We would lose between seven and eight hundred thousand would just go to where the water was, or if this took place in other states, there would be mass migrations coming into the state as well. That's what we're working on. That's what we're doing.

As far as overlapping with the feds, I'd say basically we don't have any. I mean, ever since I've been doing this, I have a lot of cooperation from the FERC. They like knowing what we're doing. They like exchanging information, and they've been a huge support. But aside from that, I like receiving intelligence briefings. I like what's going on, but until that calamity strikes and we have to do emergency management with FEMA and so forth, the states are largely on their own.

The provision of emergency services does not come from the federal government. Where does it come from? Every state has a clause that allows its governor to, in martial law, seize facilities, take over a refinery depot, deliver diesel fuel to a hospital to those kinds of things. So that FEMA will help you recover but the management of this after a short period of time is in the hands of the governors, and that's why we, in the states, are trying to get our act together and become more active, not only

prevention, but also in recovery. Thank you.

MS. BROWN: Thank you. That was excellent, excellent information. I'm now going to make a call for questions if anybody has any questions. Okay, Paul?

MR. HUDSON: So my frame of reference is from a competitive market's perspective. I think Carl and David and Arthur clearly talked about public utilities and utilities repeatedly in your presentations. But last I looked; we've got an extraordinary number of distressed IPPEs attached to the system. At the other end of the network you've got this outgrowth of microgrid activity and others that are connected to the network.

I wonder if you could just speak to how the DOE and how the National Labs and others are addressing those sort of nonregulated actors and their proliferation of nonregulated actors kind of touching portions of Tom's network, for example?

MR. IMHOFF: I'll go first. So the Department is well-engaged with investor-owned as well as the public utilities working with the

NRECA and APPA. So they cover the full scope of the utility population. Vendors are very much engaged in many of the validation efforts, field validation efforts, there are industrial partners. Typically it's 50 percent cost-share. The vendor community is very much engaged and I would argue that same vendor community is touching a lot of third-party IPPEs and other entities.

And the other response I had mentioned, Paul, Paul is that correct, Paul? Is when it comes to microgrid issues, the DOE has a substantial engagement with microgrid development, with controller development, security issues around microgrids, working with the states in terms of tools to help assess and value and look for investment strategies, for instance, remote communities and rural areas in Hawaii and Alaska and other places.

So for some of those distributed resources that are separate on the customer side, or separate from the utility organizations, DOE does have a strong basis of engagement with them

on microgrid activities that benefits from some of the cyber issues. So there are touch points. They may not be connecting everywhere, but through the vendor and the third-party IPPEs get touched. They are involved in demonstrations and DOE has a very rigorous microgrid agenda that does get into the third-party provider community as well.

MR. NICOL: So we're interested in microgrids in part because you think this is one vehicle towards resiliency as you distribute the generation capabilities, and so then the questions become related to the trust that you have or the resilience in connecting them together on and off, or have a microgrid connecting to the main. And so we have, I'm thinking of one research activity in particular that's looking at issues ensuring that commands that are used to engage or disengage the microgrid are sensible in the physical context in which they're being issued.

In short, whether commands that might be malicious to cause harm are being issued and you can check and say if I were to do this what would

happen? This doesn't make sense in the context of the state right now. And so it's, I think, an emerging area for research and not neglected.

MR. HOUSE: Just three points from our perspective. I talked about the regular utilities. Micro is terrific. It's decentralized, and a grid goes down, things go down, you've got a microgrid somewhere, terrific, all the more resilient you are.

There's also a discussion going on about nuclear power. Two crosses that and one is environmental that it does not leave a carbon footprint. It's clean, and secondly, it is not because it is self-contained that if you cut a pipeline you still have electricity being pumped out. So there is both an environmental and a security argument made for it.

Two other points, one is in looking at the businesses in Connecticut, the defense industry was by far the most resilient. Why? Three things. They screen their employees. They always have but now they screen them very, very

carefully for all kinds of things before you go to work at Electric Boat, or Sikorsky, or United Technology.

Secondly, they have to have a need-to-know to work on a particular area which is just not the case in other businesses. Secondly, there is an association of about 70 defense contractors, the big ones, Lockheeds and so on, and they meet every so often, and they exchange threats with each other. What are you guys finding? What kind of cyber threats are coming in to you? What sorts of risks are you facing? What are the new ones? And they collegially share that information.

Third, there is a structured way in which, excuse me, the defense industry can receive threat information from the intelligence community in the United States. So you got it from your employees coming in, from the bottom up, you've got it horizontally with other companies, you've got it coming down.

Now we've got to get to that state in

utilities. Now it won't be the same but of lot of utilities, they don't do background checks on people if they hire people. They don't even -- whatever. I talked to one independent system operator about cybersecurity, and I said how do you ensure the safety of your personnel? They said, oh, we got it covered. Don't worry about it. I said, I know, but what do you do? We check police records every two years. And I said I've never heard or met a terrorist with a police record, and he looked at me like I had just insulted him which I guess I had. But I mean, my point is that utilities do not do background checks and so forth to the extent that is necessary.

They also have to have access to intelligence. Right now utilities, even a couple of people go up to the secret level. They know when you talk to utilities, they know that they don't -- they aren't cleared to learn what's going on and they want to. And there's got to be some way that that takes place. We're doing an awful

lot of ad hoc intelligence briefings with the utilities here in Washington, a one-off, to tell you kind of what's going on, but the flow is not structured.

And finally, I'd just say this that in today's political climate, it is becoming more and more difficult for a politician to say I don't know. If you ask a governor how's our state? What's the state of our cybersecurity in our, you know, he can't say it beats me or she can't say beats me. You go to a legislature, the chairman of the committee and saying what is your committee doing to oversee the cybersecurity strength of our state? She cannot say I don't know.

So that's one of the reasons I was asked to do the strategy and the action plan because now what they can say is I receive an annual update summary briefing of what's going on. And according to the last one, it's seven pages long, I can give it to you, but a rigorous review did take place and this was what they found.

MS. BROWN: Thank you.

MR. HUDSON: Can I follow-up, please? Maybe I didn't ask the question in as nuanced a way as I might have because the fact is trying to do things from a top-down perspective from DOE or a public utility commission I don't think touches some of the actors that I'm talking about. And some of the actors that I'm talking about are thinly staffed; the IPP community has been stretched financially for probably five or six years now. And I think that there are some significant - call it holes - in touching many of those actors out there. And perhaps the vendor community does a good job in kind of cross-communicating, but I think that there is a gap.

MR. HOUSE: I got it. Let me give one thought on that and my colleague can respond. Yes, I think you're absolutely right.

I think that for businesses in general, but especially for businesses with a security dimension, one of two things is going to take place in the next ten years. Either we're going

to have cybersecurity audits the way we have financial audits, or there will be some kind of public-private partnership such as we formed in Connecticut. But because those gaps exist, and because the companies are not right now called to report on them, they continue, and they bother people.

So I could foresee, for example, just as you have a financial audit, and if you're a big company, you get KPMG, Peat Marwick, or Deloitte & Touche. If you're a small one you get your local accountant, but we can't go in and examine the finances of a company. But we can get an auditor's opinion, and I think the same thing is going to happen in cybersecurity that there will be cybersecurity audit firms that will come in and will review across the board, gap, the personnel gaps, the system gaps, the software gaps, the corporate culture, and can issue a letter of opinion as to how they are.

Whether through voluntary work and cooperation we can get there, or whether it will

be decreed that you have to have an audit, I don't know, but I very much agree those gaps exist and they're serious.

MR. GRIECO: Just to follow up on that, I think the insurance industry is also looking at ways that they can help assess the risks for those individual entities, and tie that to a broad range of activities in the insurance space itself that I think can help with some of those things. But I would also highlight particularly microgrids and those other distributed systems, they create interconnection points, and just the same way you think about how they're connecting from a power perspective into other systems, larger networks, other networks and look at and defining what those interconnection points are crisply and understanding how they would impact the power generation and the other characteristics of power, the communications side and the cybersecurity side needs to be thought about in a very similar way.

Those provide boundaries for you to look, monitor, understand, and really control

what's going on. That notion of federation in the communications infrastructure I think is a very similar one that could be applied to this problem of distributed systems in the power infrastructure.

MS. BROWN: Thank you. John, I'm looking at you from a time check perspective. Do we have --

CHAIRMAN ADAMS: I propose we run a little late on this one if that's all right with the group that I think this is a very useful discussion.

MS. BROWN: So we can take the questions on the table?

CHAIRMAN ADAMS: Please take the questions.

MS. BROWN: Yeah, and so, John, I think you're next.

CHAIRMAN ADAMS: Well, I have a whole series of them so any time you want to cut me off, my very first one I'm going to address it to Carl. You indicated that we needed to bring the IT

security together with the operations group. I've been noticing that, too. Operations is kind of in a silo away from cybersecurity, and although I've actively been trying to get us briefed, I'm really not quite sure why I'm doing that. Is there really a need for the people operating the grid to know about our attacks?

MR. IMHOFF: I think it's more an issue of the enterprise awareness of the overall risk profile and understanding what risks are seen on the IT side and the OT side. And there are some common issues in terms of tools and analytics that can work on both sides as well.

So it's more of a leverage and having a comprehensive sense of your risk profile. It's not that there's interconnection physically between the operations and the IT side. It's more of as an enterprise are you managing your entire risk profile effectively? And there is some opportunity to leverage from each side to be more effectively at the integrated holes.

CHAIRMAN ADAMS: I'm just going to be

sure I understand that. So we're not saying that the operators controlling the grid have to be in the loop on the day-to-day cybersecurity issues as long as the management that controls both of them is being sure that the risk profile is being controlled?

MR. IMHOFF: That's my sense.

CHAIRMAN ADAMS: Okay.

MR. GRIECO: If I may?

MR. IMHOFF: Go ahead.

MR. GRIECO: I can tell you we've seen very specific examples where people have taken the OT operations center folks and put them with the cyber operation folks. And just pragmatically the activities that unfold on a day-to-day basis are the people monitoring the IT security systems see some alert somewhere in some IT security systems. But they don't have any context of what it means most of the time, and the context of what the implications of that might be on the OT side.

And that human interaction between that, between the two organizations, is what we've seen

of the most value when you bring those two bodies together. It's not about operationally tying them together in such a rigorous way. It's about sitting them next to one another where when the IT security alert goes off there's someone on the OT side that you can sit there and say what could this mean? That has -- I'm aware of two utilities that have done that and done that very successfully.

And one of the ways that they measure it is mean time detection, mean time to repair of cybersecurity incidents that are happening in that. And that has helped them understand what's most important and what they should tackle.

MR. HOUSE: I'd just say absolutely. I mean, absolutely IT and operations technologies have to be brought together. There are some utilities who say the more important of those two is the operations but we need to keep the IT folks informed; that kind of to put it backwards and huh.

Look, we just heard what happened in

Ukraine. They came in through the IT system, jumped over to operations and shut it down. I mean, if ever there were a case study laid out for the world to see that operations technology and information technology are just part of the same cybersecurity thing, it was demonstrated for us right there. So I think the answer is absolutely.

There are people out there right now who are saying cybersecurity is not an IT problem. It's an operations problem.

MR. NICOL: And if I would add I agree with everything that's been said and add that the problem is worse than stated. That on the operation technology side you can have some siloing as well. You have the networking people who aren't talking to the IT people who aren't talk to the security people who aren't talking to the compliance people, and so things fall in-between the gaps.

CHAIRMAN ADAMS: You know, I've got a much later question but I'm just -- because you brought up NERC, is the NERC, and I'm really thing

DOE communications, National Labs communications, is that good at the moment?

MR. IMHOFF: My perception is it's very strong.

CHAIRMAN ADAMS: Good.

MR. IMHOFF: They're --

CHAIRMAN ADAMS: That's all I need to know. Carl, you had a list of fundamental research one through I'm not sure how, I got down seven and with slides. Was that prioritized?

MR. IMHOFF: No, it was not.

CHAIRMAN ADAMS: It kind of --

MR. IMHOFF: It was not prioritized. It was just a smorgasbord.

CHAIRMAN ADAMS: It would be worthwhile prioritizing I think.

MR. IMHOFF: Was that a request?

CHAIRMAN ADAMS: I think it is more important than the Labs and DOE have that prioritization than I have it, but right, I mean, laundry lists are difficult because we can't do everything.

MR. IMHOFF: Well, that's why on the next slide I tried to winnow it down to the four, what I felt were the priority areas on that next slide.

CHAIRMAN ADAMS: The key questions which --

MR. IMHOFF: At the bottom of the slide, the technical or S&T priorities.

CHAIRMAN ADAMS: We talked about, you know, we need to design the architecture with resiliency and performance. This was actually David's comment. I'm sitting here going, well, are there commercially available systems that are designed for both performance and resiliency? And in my mind, I'm thinking resistance to cyberattacks when I'm hearing resiliency. Are those available today? Can I go out and buy one?

MR. IMHOFF: There are systems today that are newly designed for, like, DERMs applications and other things. They reflect, I think, today's resilience attributes, sort of best practice for today. But I think they fall short

of what the system is going to need five years from now and ten years from now.

I think they are -- so they are moving in that direction, but I think there's some fundamental opportunity -- they are basically doing today's practices in a more secure fashion. But there's an opportunity, I think, to look at tomorrow's practices that are inherently more resilient and those are not yet available to my knowledge. Others might disagree.

MR. NICOL: No, I won't disagree. The systems are designed for performance. That's something that people take -- expect but they're not expecting security, and so systems tend not to be designed for that, and it tends to be an -- there are exceptions of course, but I think as a trend, it's not there.

MR. GRIECO: I would just comment too that the resilience conversation to me is very similar to the defense conversation. It is one in the cybersecurity space that will continue to evolve. The state-of-the-art for today for

resilience will need to be evolved in the next five years.

We've seen that in the communications infrastructure. It will be consistent across all domains that cybersecurity touches. The things that we did ten years ago to make a product resilient pale in comparison to what we're doing today because of what we know the attack surface is, what adversaries are doing, and what the risks are.

So I think one of the important kind of twists here is resilience is not a destination. It is a journey and you will continually be on it and need to be thinking about it consistently.

CHAIRMAN ADAMS: Well, as part of that journey, yeah, I worked for an ISO. We had new IT systems every week. In fact, I've had a statement made every day. Is there a checklist for our project managers that hey, we should be checking off that penetration of this system will be inherently limited in our exposure? Does that checklist exist? Is there something y'all can

hand me that I can take back and say we ought this to our project management flowchart that we are examining for cybersecurity.

MR. GRIECO: So I would comment that there is a set of best practices that should be a part of any project assessment that you're doing including risk frameworks that can help you think about the National Institute of Standards and Technology (NIST), the Cybersecurity Framework is a great way to think through risks inherently within a project itself. There is no magic checklist of if you do these five things you are secure.

There is a checklist of things that will help you make sure that you understand the risks that you're taking on from a cybersecurity perspective. And that can be mixed into your overall business and technological approach to what you're doing.

MS. BROWN: John, if you don't mind if I could jump in and ask a question that builds off of --

CHAIRMAN ADAMS: Sure.

MS. BROWN: -- and that is, Your Honor, I think about it from a communications perspective. I think there is the intent to build and design it such that it sort of has future proven capabilities. You know, that it can scale, et cetera. And I'm just curious as you look at what's being designed today or systems that are designed today if they factor in, and maybe what are the elements so that they have the capability to adapt for kind of future issues.

MR. GRIECO: At least from our perspective on the communications side there is a focus in two major areas. One is foundational security capabilities that provide resilience at a really elemental level that provide an ability to recover, an ability to defend. And then secondarily, there's a flexibility being built on top of that foundation which allows for resistance to defense that is indeed in many cases programmable. But again, I would encourage the thought process here to be one of this is going to

evolve as adversarial activities evolve and threats evolve.

MR. IMHOFF: Just a really quick response. The grid architecture research is looking at an issue where today most new distributors source concepts, or outage management concepts, or other things they bring with them their own communication functions. And they're looking at in a highly distributed world, are there better ways to build communication layers that will they be more effective at being able to be made secure and will it be easier for regulators to rate-base get cost recovery for that core communication layer that will serve multiple functions in a distributed utility future.

So there are considerations of new business models that would provide more inherent upgradability and future flexibility.

MS. BROWN: Great, thanks. Okay. Mladen?

MR. KEZUNOVIC: Okay, well, this topic is fascinating. You know, there's never an end to

it, and I really enjoyed the discussion. You know, the priorities are always an issue. It's not that you put the right priorities, it's that you have a priority and they are right, you know. They always have something else.

So I would like to make a comment about the priorities and obviously with a view of DOE, not the entire world out there. One priority is the cyber physical security and why I'm adding this physical part because those two interact. And that is not explored to the extent it needs to be explored. You can bring the system down by messing with generation, messing with load, inducing folds, which is all subject to malicious events easily.

And at the same time, do something in the cyber area, and it becomes extremely complicated to detect, because all we care is at the end of the day is detection. Okay? Because you have to know that something is going on before you can do anything about it, right? It gets really complicated.

And there's a lot of research out there, there are a lot of demonstrations, this and that, but I think the space for DOE in that area is still solid. So and that would be -- that's my opinion. Now I would like to hear back if we have the time, if not, that would be my recommendation if somebody asked me tomorrow.

The second part is the open source software. As much as open source software is a vehicle for innovation and whatever else it is, you have to put it in a context. We come into an industry that is not used to it, and has to get used to how to verify open source software and how to deal with it. How to distribute it, I mean, the word says open source software. I'm going there. I'm getting a license for Berkeley license or whatever other license, do changes; put it back in, what is the mechanism today that exists within the DOE or anybody else to think about how to deal with all of this?

And so that's something that is being done by DOE entities at the moment, being promoted

by the DOE entities at the moment, so I would ask the question how that is going to be secure? So that would be the second comment.

And the third one is something about security by design, okay, by design. And what I'm referring to and everybody else mentioned this and not only here but everywhere else, the legacy systems are there for 50 plus years. EMS and other stuff is there forever, okay?

Yes, we change them every, you know, 15, years with the new technology, this and that,

but conceptually they are the same, right? So if I were to learn about how these things operate, I have plenty of history of how I can learn they operate, and how I can mess them up. And they are vulnerable by design because when they were designed, cyber security was not the issue period.

So you know, DOE can have a role in advancing the new concepts of design, security by design. And I don't need to go into how this can be done. There are plenty of ideas how this can

be done particularly we are adding things like these microgrids and (inaudible) and whatnot, what is relatively new, but also with the grid itself. So that would be another third recommendation.

Now you know the time is a factor here. It would be nice to hear back but if we can't hear back this is not questions. This is straight comments, okay?

MS. BROWN: I'm looking at John to keep me -- time for a response?

CHAIRMAN ADAMS: Yes.

MR. GRIECO: So I'll comment on two of them. The open source software comment is a really important one. I would encourage thought here that the power vertical is not the only one grappling with the open source software and the security implications of it. There are models that can be looked at that I think do a really good job of managing risk.

I think there's also a real role that all of you all in the room play in the context of procurement and ensuring that as a part of the

requirements that you are issuing to vendors that are providing you capabilities that those risks are also managed upstream of you when you procure or buy equipment or software that may be using things such as open source or others.

And that goes to the second point of involving security by design. Again, lots of talk about that in other verticals that can be leveraged in the context of it, it's the same statement though. A lot of this has to come from the procurement side to make sure that those are requirements as a part of what you will buy and when you buy it, you expect those sorts of capabilities to be built in.

MR. HOUSE: Just two quick points. One is open source software is open and it's open to good guys and bad guys. And somebody who gets an open source and can start doing some work in how to penetrate it, so if I were going to use an open source, and I were in charge of cybersecurity for a company, I'd say that's very good.

Now this is open. The whole world knows

about it. What have you done to make it safe for us to use? Secondly, DOE role, I mean, I come back to the fact that this is the federal system of the United States.

DOE itself does not have a role to play in the states which are major factors here. I think the collaboration is excellent. I think -- or can be improved. It can be a resource. The fact that I was invited here today to talk about things that DOE does not do indicates that there needs to be communication and rapport.

But in discussing what the DOE can do, please don't fall into the assumption that that solves the problem for the United States. Unfortunately, because of our federal system it's far more complex than that and you've got a whole lot of individual players out there some of whom aren't doing a darn thing about cybersecurity. And as long as that's the case, then the United States does face a vulnerability.

MR. NICOL: So you'll find you have an ally in me on your first point. I think that the

area of looking at a combination of a physical and cyberattacks to cause bad things to happen is underserved. One of the great risks I think with cyber is the possibility of doing coordinated attacks at places that are distributed. This is what makes it different from tornadoes and hurricanes and things like that.

And so if you have a distributed, coordinated physical attack, and then deny situational awareness on the cybersecurity side then you just put the system in a state where it's going to chew itself up. And so I think that that's a good area to look at.

Open source has been talked about. We're very much in agreement that security by design is important and we're working on that. I think also it's important to, you know, we have legacy systems and for the next 20 years you'll still have legacy systems. And to be able to protect those somehow, and so I think that on that, that's an area that needs attention as well.

MR. IMHOFF: Just quickly, Mladen, the

issue of cyber physical is what I was alluding to in terms of the solutions have to have the full system perspective, and we need to look at the impacts of IT and OT cyber responses and how they impact things like control and protection. You know, everything's connected and the protection relays and others are great examples of piece -- components that would be very much involved in a cyber physical sort of engagement. So I think that's how you would mitigate some of those issues by making sure you take that broad systems impact across the entire system and look for the full consequences.

In terms of open source, I think open source is predominantly an early innovation trigger. Utilities rarely use open source. They -- typically it's picked up by vendors and we're working with vendors now so that as they -- we try to build in as much design for security into this open source tools, but then we work on the handoffs such that the vendors can then take that and embed within the protection of their

commercial products. So because it's a very important point and it's one that's being considered and worked on to mitigate as best we can some of those risks so.

MR. KEZUNOVIC: I just want to make a comment for record that, you know, when I talk about the recommendations to DOE, I assume that DOE exists. What I mean by that is I'm not trying to suggest whether somebody at the state level should have that responsibility or somebody at the federal level should have that responsibility. The point is DOE exists, DOE has activities, and what I was talking about is a suggestion that those activities could be covered.

Now how someone takes experiences out of all of that into the environment that is a state environment and a company, private environment is kind of a different discussion. It is the knowledge issue and demonstration issue that matters. And the resources, there are state resources, as far as I know, on some of these topics, don't simply have neither financial nor

human resources to address these issues, to learn, not to take action, to learn. So that's -- I just wanted to put that on record because this is going on record.

MS. BROWN: Thank you.

CHAIRMAN ADAMS: I think we've run out of time.

MS. BROWN: Yes.

CHAIRMAN ADAMS: I really thank the panel. I could continue this all morning but I think we need to take our break and reconvene around 10:30. I want to thank the panel very much, very enlightening, thank you.

MS. BROWN: Thank you.

(Recess)

CHAIRMAN ADAMS: I'd ask you to take your chairs now. I put us 30 minutes behind so I'd like to try and get started. We're now going to turn to Hank Kenchington to talk to us about the draft multiyear plan for energy sector cybersecurity. Our Smart Grid Subcommittee under Paul was asked to review this draft report back in

July. So we're also going to take a few minutes after Hank to talk about that informal feedback that we shared. Don't have any slides I'm going to put up on that. Just going to talk to through what we said because it wasn't official. It was informal.

And then with a little time, I hope we'll get -- ask Members to share your thoughts about specific topics we might want to explore on this, whether or not there's anything further for us to do. Hank, thank you for coming and giving us this briefing.

MR. KENCHINGTON: Thank you. Thank you, sir. Thank you all for having me today. I appreciate the opportunity. First of all, I have to say, John, I got quite a stir coming in the door this morning.

I came in at 8:01 and you all apparently had started promptly at 8:00 and I looked at you and I said, my, I didn't know Secretary Perry was going to be here today. And I was like, oh boy; I'm going to have to change these slides. I mean,

am I right or am I wrong? Huh?

CHAIRMAN ADAMS: It's the glasses.

MR. KENCHINGTON: Okay, thanks. Okay, so my name is Hank Kenchington. I've been with the Department since about 1995. I've been involved in cybersecurity for energy systems since about 2005, so about over 12 years now. I started a program we called National SCADA Test Bed at Idaho in 2005. We got some finding and been working with the sector ever since, more involved in some years, less involved in other years.

But kind of just to give you a perspective from the Department, so kind of where we're coming from, I'll just share with you a story from the -- of the previous Administration. So there was a general, one of the generals on that was NSA or CYBERCOM, was up on the Hill, and he said something like the Chinese are all over the power grid. They're all in the power grid.

And I don't know if you all remember, this is a true story. So this kind of rattled around the press for a while, and then it got to

public affairs, and then, you know, Congress got it, and they started writing letters, and questions started being asked, and then it goes to the White House. And the White House asks and the White House says, and it comes to the Deputy Secretary, and they say, DOE says, how secure is the power grid? Do we have a problem or not?

And that floats down to Hank. So I'm like oh my goodness, I guess so, so the National Security Council is calling and they want to know. So I gave them, you know, the first answer was the attorney's answer right? It all depends, right? It all depends on where you look, where you look. So I got -- that wasn't acceptable of course. No, we need to know. But if you really think about that, you know, that if we have a massive, a large outage even today it goes to top authorities. It goes to the White House. It goes to the Secretary of Energy, and the people are pointing the fingers down, okay, so I'll just share that with you.

But what they came back was so we -- this is from the National Security Council, we

would like for you to hire the Department of Defense to go out and do a red team on the power grid. We want you to go find out and hire DOD to go look into all these systems and tell us are the Chinese in these networks.

We're like whoa. So what do you say? Well, how do you go back to the lighthouse and I'm like well, I don't think, you know, the -- let's say the EPBs, the Electric Power Board in Chattanooga or the municipals or the people who -- the private sector owners and operators who actually run these systems, they may not like that. But of course the White House doesn't want to hear that.

So we say, well, what are you actually trying to do? Well, what's the point? Well, you know, we actually want to make sure that the grid is adequately protected against cyberattacks. You know, we just want to help and we want to improve the -- if there's a hole, we want to fix it. That's what we want to do.

So I thought, well, how about a maturity

model? How about if we developed a tool that would help utilities asses their own system, identify where they have holes, and help them identify what their priorities should be, where they should put their resources, and actually benchmark against their peers so we can get this kind of a market peer-driven way to enhance the security. What do you think?

And after many discussions, yes, so that's where the cybersecurity capability model came from if anybody really wants to know. So that was the evolution of that. We developed that model working closely with the sector in about six months and actually piloted it at about

utilities to come up for that model. That model's being used today, APPA, NRECA, they're using the model going out to help utilities actually assess their performance themselves, identify where their weaknesses are, and continually improve.

So that just kind of gives you an example of kind of where we're coming from and

just, by the way, then this framework that's so popular, was the result of the capability maturity model. So that actually -- so why don't -- it was, okay, this was so successful in energy, why don't we do this across all sectors? So that's NIST's responsibility and they developed the larger framework which is now applicable to all.

So be that as it may, let's move forward to multiyear plan. So how did we do this multiyear plan? First of all, we started working with the -- do I have control here with this? Ah, there we go.

So I actually got involved in 2005 and started talking to utilities, started talking to vendors, what are the challenges? I came from the private sector. I'm a customer-oriented results-focused kind of guy. And I said well, maybe we should talk to the people actually that own and operate these systems to find out what the problems are.

So when I talked to the utilities, the utilities were okay, well, these vendors guys they

don't make secure products. The products are terrible. They're awful. I said, okay. So we talked to the vendors saying the utilities say you don't make good products. You've got wholes in all your products. And they said, well, they don't ask for security. They don't want it. They don't want to pay for it.

So I went hmm. Where do we start? Where do you start in this whole circle? One guy is blaming this guy. This guy is blaming that guy. So where do we start? So we actually started testing systems at the National Security test but it was clear from the beginning, is the point I wanted to make, was that there was a public-private role here.

We have a shared responsibility. There's a point, I mean, our philosophy, and I'll talk a little bit more about it when we get into the plan, the private sector runs and operates most of the majority of the energy infrastructure, have the primary responsibility to ensure that their systems are adequately protected. Now

shouldn't we expect the private sector to be able to protect against let's just say a nuclear incoming warhead missile from wherever? Should we hold them accountable to protect those systems from a nation state?

In a physical world one would usually say no but is -- can we take that same logic over to the private sector and say, well, are we holding these utilities, the asset, the owners, the energy sector, the oil and pipeline operators accountable for protecting those systems against the nation states? Does this make sense?

Where is the public -- where does the government get involved? When does it become a national security issue and when is it still a private issue. That's I think are still open for debate. But so we developed a working with the private sector, so we have two groups involved, public-private. What are we going to do?

I mean, if we have to work together we need to be going to the same place, right? So who's going to do what? You're going to do this,

I'm going to do this, and we're going to have a plan. We need to have a plan. We have a plan. We need to know where we're going. So we pulled together a group back in 2005 and put together this roadmap. We updated in 2011, but in the roadmap we called for this vision here, resilient energy systems designed, installed, operated, made a survivor incident while sustaining critical functions security designed in which is what the gentleman spoke a little bit earlier I believe.

This was in 2005. 2005 these guys were asking for resilient systems. So they're calling it resilient systems before resiliency became this government buzzword. So who put this together and who pulled together the vision?

Well, I'll give you the groups. I won't call out the names. Who participated in coming up with this vision? And it's an electric institute, ERCOT, independent electricity system operator Ontario, British Petroleum, BP, El Paso, Ergon Refining, Progress Energy which is now Duke, NERC, DOE, Alyeska Pipeline, DHS, and Entergy. So this

was an industry, public-private group coming together to put together this vision. This is still relevant today.

We've been using this for the last 10, years to guide what we do. We have, this is great, you can't see anything I got here. Okay, but give you a sense of the milestones, but if you're going to make a difference, you've got to have a plan. You've got to have a way to measure your progress. You've got to have a way to measure your performance, are we making a difference, or not making a difference? You need to know where you're going and you need to work together to do this.

So this is the tool that we've used, been using. We did an analysis, and I get a little bit -- you can't see this either. I apologize, but we currently have about 48 projects underway and one Dave Nicol with the National Labs and with the University of Illinois, Cisco is involved in some. States are involved that address some of the priorities in there.

We've actually commercialized over 30 technologies as a result of this that are out being used today in all 50 states to help better secure the system. There's new tools out there that are available, that have been made available over the last ten years. C2M2 is one. Failure scenarios, which was developed by the Electric Power Research Institute (EPRI) which DOE funding through the National Electric Sector Cybersecurity Organization Resource (NESCOR) is another great document that actually gets to the process of how to -- what security controls are needed to adequately protect that AMI smart meter system. Do I need to encrypt that data or not?

Does it need to be authenticated or not? How do I do it? What are the requirements? So we've came up with tools that were not available ten years ago that actually help you design in the security. So but the situation's changed. The technology landscape has changed. The energy landscape has changed. The policies have changed. We have the CISA Information Sharing Act came out

last year, FAST Act came out designated DOE as the SSA, our policies have changed, even our thinking, and in particular, the threat has changed.

The capabilities of our adversaries has significantly grown. We particularly in control systems, this is a little timeline that focuses just on control system attacks. It's not -- we're not -- Equifax is not on here today, neither is Target or Sony. But when you look at what's happening from the Stuxnet to Metasploit to the availability of tools that anyone can download online to exploit these systems online, it becomes much easier for an attacker to make an impact.

And in fact, nation states who don't have a whole lot of money, small states for a few thousand dollars can hire people. You don't have to -- we used to have an intel model that we measured people's capabilities, their intelligence. Well, they don't have the capability yet. Let's talk about Korea.

They don't have the capability to build this missile and all of a sudden, boom, they do.

What happened? It used to be well, they're going to need to make smart people. They're going to have to develop these smart people. That world is over.

The game has changed. As I said, the technology landscape has changed. We have much more distributed net generation, we have these endpoints now that how do we protect those with the same kind of protections that we need for the bulk power system. How do we get that to the distribution level? How do we get it to smart meters? This whole how do we do -- this whole system of systems, the IT, you go after digitalization, everything these guys have said is true. And we're not going to stop digitalization because the benefits are too great. Economic benefits are just too great.

We've got to find a way to manage the risks. So about a year ago, well, let me back up a little bit. I want to make the point that, and go back to Tony from Cisco. He said the game has changed, and I totally agree with him but maybe

for a different reason.

If we look at the breaches, look at how much money is being spent on cybersecurity, and how much resources are being invested in cybersecurity today, it's growing at about a rate anywhere between 8 to 15 percent. Our GDP is growing from somewhere around two to three percent. Cybersecurity resources is generally, except for the companies that build things, a nonvalue-added service. So there's going to be a point where the costs, we're not going to be able to afford all the protections to get the benefits that they provide.

So we have that point. The other point is the defend -- we have a totally asymmetric ballgame here, right? Meaning that the defenders have got to be 100 percent correct, right? They've got to be able to patch every hole, and the bad guys just have to -- all you have to do is click on one link and that nation state is in the PJM and all of a sudden, or not PJM in particular, but any entity, all of a sudden, they own the

system, one click. Click a link. One link and they win.

We are in a game we cannot win, right? We got to change the game. Change the rules or change the game. So about a year ago, we started rethinking the way we -- what we were doing, are we organized properly given this changing landscape? Are we working on the right things? Do we have the right people working on the right things?

Have we -- are we leveraging the full capabilities of the Department? The Department's very unique and that we have ownership over I think 27 national laboratories. That includes things like at Oak Ridge is a spallation neutron source that provides services to around the world which is nothing really more than a process control system. But we give access to people around the world so we have control systems.

We monitor these networks. We have the world-class cryptographic people, the National Labs of scientists, the -- are we leveraging on

that all to the best that we can? And we're a member of the intelligence community? Are we bringing to bear our relationships, our connections back with the high side and the intelligence community, with the FBI, DOD, DHS, all those folks? Are we bringing that to bear to help solve the problem?

So that's kind of the basis why we started rethinking what we were doing. Out of that came this multiyear plan. I will say it's a draft, okay? And I'll explain maybe a little bit why but what we are now, I won't say in the middle, we're at the end of getting comments. We did get comments from the Smart Grid Subcommittee, thank you very much. And they were very thoughtful and I will take a minute to thank personally Paul Centolella.

But so we are taking comments on that but -- and in driving this forward, this is kind of the process that we've used. We took that roadmap. We did an assessment. We had a National Labs. Each one of them go out and meet with their

reps around the country and the private sector folks are already making progress to collect data. Have we really made a difference on that roadmap?

And that's -- what we found is in the plan that we can share that we made some significant strides in some areas, and in some areas none. I think one area where we made a big difference the last ten years is executive engagement. Ten years ago it was all the technicians, the operators, those cybersecurity guys that said this was a problem. Now it's the CEOs that are saying it's a problem, okay?

We've got that engagement. There's a number of tools, better tools out there to help utilities design the security. There's some advanced technologies that are out there that are making it easier that actually are more secure and cost-effective. So we have that list and we use that to help inform this plan, this multiyear plan. The plan is the Department's plan of what we think we can so in the next five years in this whole space.

As I said it's a public-private partnership. We have a role. The utilities have a role. The asset owners have a role. FERC has a role, NERC has a role, EPRI has a role. They all have a role in this but we wanted to be clearer about bringing to bear the assets of the Department and trying to address this problem.

So as you can see the energy, the sector's needs feed into our plan. We have other policies that we have to address. We have priorities we have to address, and these fed into these as well.

So and as the gentleman said earlier, you can't make a difference unless with all these things going on unless you prioritize. So how do you prioritize? We're taking two basic legs to this. First is we've got to win the game today. We need to be able to better protect our systems today, be more prepared, improve the way for preparedness through exercises, better share information in real-time, machine identify these threats, and protect today's systems.

But as I said, that's a game that we can't win. We've got to change the game. How are we going to do that? Well, longer term research and development, let's invest in the right things to find ways to help change the game, and I'll give you some examples of things that we're kind of working on now that are close, and approaches that we've been taken that may help us change the game a little bit.

So we have those two pathways and our goal is one, strengthening preparedness through information sharing. We want to help look at the supply chain risk, at the vendor risk. Number two, better coordinate how we respond because we will need to respond. We've already had to use this in the last six months. How we respond because there will be incidents, and so in game-changing R&D working National Laboratories, academia, industry, everyone who can contribute something to the ballgame and find a better way to do this.

So I'll just go through a few examples

of our goals. I will say we've shared this now with the electric sector coordinating council. We've gotten their comments. We shared it with the oil and gas sector coordinating council. We've gotten their comments. We've shared it with a grid lab consortium. We've gotten their comments. We've gotten comments from the EAC Smart Grid Subcommittee and we've integrated those.

I'll just say some of them are very, very thoughtful. Much of them was a little bit out of our scope. Not much, some were out of our scope, but they really didn't change what we're doing. No one really said that you're doing the wrong thing, your focus is wrong, you should be doing over here, you shouldn't be working on this, you should be doing this, and those were the questions we asked. We didn't ask can you please edit this document? We said are we working on the right things? Should we be working -- are these the right priorities for DOE? And so it came back we were pretty much I'd say 99 percent final with

those comments, and these are the priorities that we've been able to lay out.

Example, well, hang -- there we go. CRISP's cybersecurity information sharing program, this is a program that leverages work that was done by DOE starting back in 2003. We have sensors on the DOE networks across all the DOE labs, goes into to two central points. We're looking at that data, looking for attacks.

2007 we said, hey, why can't we leverage the same capability with the private sector? Sounds easy, why not? Let's try it. Took us seven years to 2014 to find a way to address all the privacy issues, all the information sharing issues, and now it's being managed by the ES, the electric sector, ISAC, but they provide through PNNL who is working with them to provide some of the unclassified data analysis. The DOE, our portion of this in this partnership is we provide the classifying analysis, okay?

So what we do is we get the data. We have our own team of analysts, energy sector

analysts, every day looking at data, looking across the IC community. What's DOD -- what's NSA seeing? What's DOD finding? What's the FBI finding? Are we seeing these same actors playing in our energy sector? So we're taking that information, declassing it, getting down, sharing it out through the ISAC, okay?

The problem we have it's very hard to show our value proposition here because reports that come out from the ISAC will not say where that information came from. So you may get an owner-operator, now you got a thing saying block IP 1.3.4.X.XX and that's all it'll say. You won't know where it's come from or how you got it. But this has proven to be a very, very valuable tool, and what we want to do is continue to improve that tool.

Right now we're working with NSA and ICITE which is called the Intelligence Community IT Environment to share this information with more, higher advanced threat analytics, and be able to do it faster, cheaper, and provide more

value back to the utilities. So that's CATT, the Cyber Analytics Tools and Techniques, share that data in real-time machine to machine with the utilities.

And CYOTE which is -- so the sensors that we have today are deployed in the IT networks, and of course, we're really concerned about the operational technology networks. Well, we have a pilot going on as we speak with four utilities to say hey, is there a way that we can get data from you guys, share it, enrich it through our classify -- what we know, classify it, and share information back? So that's one of our next steps with that. Its focus, as I mentioned earlier, some of the smaller utilities that may not have their resources to do this adequately, two years ago we put together cooperative agreements with NRECA and APPA to do four things. One was conduct cybersecurity risk assessments. These were to do hands-on, to do onsite vulnerability assessments on those systems.

You guys do it. We don't want to get

involved. We'll cost-share this with you but you run the program. You do it. We don't need to see information. You work with your two utilities and help them improve their systems. This is going on today, also to pilot emerging technologies and develop ways for results to better share information on threats.

One of the technologies we help actually within NRECA that we'll be able to deploy some information-sharing technologies, if all things work out, across 1,000 to 2,000 utilities within the next three years. So we have -- this is really working great and these guys are doing a fantastic job. We're going to continue to work the cybersecurity maturity model provided to really get this right -- you really need a third party to come in and help you do an assessment. That costs money so we're trying to support this as well.

And incident response, one of the things we did to be better able to bring to bear the whole of government, when I say that I mean, you

know, things like the IC community, NSA, DOD, those folks, when we have a challenge and what's going on out there? Do you see it? Do I see it? Yeah, I see it. Is this just a one-off? Is this a nation state campaign? What's going on? And how do we get that information from our IC community out to utilities who can actually do something about it?

So one of the things we're working on is working because you're going to need teams when things happen, to go out there and do triage with the utilities. So we're developing teams at our National Laboratories who will be able to respond to these kinds of emergencies.

And then the last category is, because it's 11:00, the R&D, the change in the game aspect. And we're looking at this from two perspectives, the legacy systems, what we can we do about the legacy systems that are out there today, and two, how do we develop these inherently secure with security built-in systems for tomorrow? So that's fundamental in the two

approaches there.

We have a portfolio projects that we've been funding for over ten years. We've invested over $240 million in this work, commercialized over 30 technologies that are out there being used today. And it's also all across the United States. But our approach is we work on the longer-term research, the mid-term, and getting it into the market, but we've got to bring the utilities into the game because we want to get something done and actually usable.

An example, this is software-defined networking commercialized by Schweitzer in 2016, last year. What they've done is, and this is actually an evolution of a number of technologies. There's whitelisting built-in, but they can also -- what it does, it provides you -- the traffic engineer, he can reroute his communications. If I have a problem here he can reroute it, or he can program it so it automatically reroutes. So I don't have to go out in the field and do this type of communications.

So I can automatically send something and detect it and go around it. This gets to the resilience aspect. How do I -- if I fail here, how do I turnover? How do I reroute to my other system? But it has to be the whitelisting capabilities which is particularly suited for the OT network. So this is designed for a substation to control center communications, but the real beauty of this and the reason why it's flying off the shelves is it improves security and it saves you money. It reduces your operations maintenance cost.

If you can hit that sweet spot, you'll greater and greater adoption. That's where we want to be. And that's why we're working closely with the utilities and the guys who actually use these things, who know the problems, who install them, who can say, yeah, that'll work or that won't work.

Another example, this is intrusion detection system that was commercialized by ACS. This kind of evolved out of the Recovery Act where

they're proving an intrusion detection for wireless, for AMI, and for DA. It's kind of the security layer for your other vendors that you're working with. This is being deployed now at least four major utilities.

This is a relatively new technology. This is getting at let's change the game, do it a little bit differently. Let's assume the IT network is going to be hacked. Assume the adversary is going to get in. Well, I'm going to leverage my power system because power flows according to known physical laws, right? So what I'm saying here is if I get a command in, ABB has done this, built it into their firmware, into their relays, their RTUs, that they cooperate. That's why it's called, excuse me, collaborative, collaborative defense.

So I get a command in my substation to go do X, I automatically go out and fast, less than

milliseconds, go out and determine well, that put me in an unstable condition or not.

Should I take that? Should I actually do that or not, okay? And then you can tell it do I want it to alarm, do I not to do that?

So this is using the physics of the grid to defend itself against an attack. This is in the process of being commercialized by ABB.

This is a little bit more of a longer-term research working with Los Alamos and Oak Ridge on quantum key encryption. The beauty of quantum key encryption is if anyone tries to tamper with it you will see it undeniably. We can use this for really critical assets. You wouldn't use this everywhere. But where there are really critical assets this could be part of the ballgame.

We hope to, we just -- one of the projects we just launched with Oak Ridge and with Los Alamos is hopefully we'll be able to build a network from Los Alamos to Oak Ridge with this technology built-in to test it out. This has come a long way that we're trying to show here is it was this big and they're trying to get it down to

this big and reduce the cost at the same time.

We are working with the National Laboratories, and I'm not going to go all through the list, and in a number of ways the laboratories have unique capabilities. Each one is unique but each one's the same in some ways. But we're trying to build kind of core capabilities at each one of the Laboratories. I know that they would each one say that this is not all I do if I just gave them one line, for example, Argonne does power systems and applications that are cyber aware. They would say oh, we do much more than that and I agree.

But we tried to get it on one slide. But we are working with them actively, and someone mentioned the projects, and we just awarded, I think they came out Tuesday? Tuesday they were announced. We are -- this kind of happened pretty fast because we're at the end of the year. Funding was a little bit delayed and we've got to get it done. So these are titles of the projects that we're working on. Some of the challenges

that these are designed to address are one -- are devices that are on the internet that are open just as the gentleman with Cisco said.

I can go out there and do a scan and find these devices and routers that are out there. They have known abilities and they're not even password protected. How do we design tools to better determine so utilities and energy sector and others, oil and gas guys can say, yep. I know I have nothing really exposed. That's one of the problems. Getting into distributed energy resources, how do I provide the security down at that level, at the distribution level?

Some of these are addressed at that. Another one is at the firmware issue, how do I ensure that the firmware on a PLC on the end is what it's supposed to be and nothing else? That's a challenge without pulling it out while it's operating. We've got a couple of projects that are going to do that. The UUDECs problem at PNNL is looking at the ICCP. We've tried -- since I remember we started a project in 2005 to find a

way to better secure ICCP which is the inner control center protocol across all the utilities. And we haven't been able to find a way, a good way to do it. PGP, PJK, I forget what the technology was but it's all deployed differently, although it is a standard it's deployed and implemented differently.

So we're going to start from scratch. Start over, start a whole way of doing it differently. So these are some of the projects. These are a little bit in flux as far as the partners. They all have industry partners. They all have laboratories. We want the -- we've got to have those industry guys involved upfront to put skin in the game because we're not going to work on things that just aren't going to go anywhere. This will help us ensure adoption at the end. So I'll close with that. Thank you. Thirty-five minutes.

CHAIRMAN ADAMS: Thank you, Hank. I want to just ask, are there any questions for Hank now? I wanted to share -- I've got the comments

that were made or a summary of the comments we gave back to you earlier. I felt like I should share them with the group. But any questions for Hank before I do so? Please.

MR. WEAVER: Just a quick question on could you speak just a little bit on coordination between DOE and DHS? Reason for my question is we spent some time this year answering questions from DHS. I think they were called the seven steps to cybersecurity. I'm sure that's probably somewhat relative to your cybersecurity maturity model. Just briefly, could you explain that?

MR. KENCHINGTON: Well, actually I think we came out with -- what was it, was it seven steps was a DOE document for SCADA security that we published in 2003? Yeah, it's available. There's a number of those but your question is really about coordinating through DHS, right?

MR. WEAVER: Yeah, and relative to the questions that came out this year after the Ukrainian incident that really were an evaluation that we could use internally and cause us to take

some actions to close some gaps.

MR. KENCHINGTON: Okay, so the Ukraine incident, we helped lead a team that went over there, okay, with the ISAC, with FBI, with DHS. So we're all part of that team and we work with them to determine, you know, what did you find, what did you see? As a result of that, through the ISAC and through some folks actually at Idaho National Lab, we developed the -- this is what happened, right?

It's actually on the ES-ISAC website right? Here's what happened, I forget what it's called. It's kind of like the DOD or used case. So we worked with them to develop that. We also worked with the ISAC to conduct training courses on what happened there and what to do about it with DHS. They were all part of the process.

But from -- I'll just say from a higher level we work through the whole -- went through the electric sector coordinating council, the oil and gas coordinating council with DHS which is under their framework. They are part of that. So

at a higher level, we engage with them and more from, I would say, from a -- I think multiple levels really, all the way from the Secretaries down and working trying to coordinate through that national infrastructure protection model where we're the SSA. They're the overarching ones.

So there's going to be some overlap. They have some resources that we don't have and we have resources they don't have. So it's trying to coordinate those is a challenge for all of us.

MR. WEAVER: Thank you.

CHAIRMAN ADAMS: Hank, I want to thank you, and I want to make something that I have been slow to recognize is your ability to plant seeds of protection. I mean, it isn't just a single thread that you're working on; it's a whole lot of seeds of protection you're planting.

MR. KENCHINGTON: Yeah, our philosophy is, you know, there's a hole here. Okay. There's a vulnerability there, yeah, okay, what are you going to do? No, we don't lift all boats. Where can we -- it's a return on investment (ROI) thing.

Where do we spend the least amount of money to get the biggest bang, right?

How do we lift all boats? What can we do to improve the security of the whole sector? It's not just about onesie-twosie. If we focus on onesie-twosie we'd all be nuts, more nuts than we already are.

CHAIRMAN ADAMS: Thank you very much.

MR. KENCHINGTON: Sure, thank you, appreciate it.

CHAIRMAN ADAMS: At this point I'm going to go up to the podium and share what was fed back at least in summary. And I'll turn over the chair to Ramteen for a few minutes. Thank you.

CHAIRMAN ADAMS: First, I want to give credit to this to Paul, who led the Smart Grid Subcommittee, gathered comments, gave feedback, and was recognized by Hank. I'm going to be very brief. Paul wanted to point out that the threats to the power system are dynamic and asymmetric and that the operation of the power grid requires stability which is nonlinear. Actions impacting

frequency or voltage could disrupt operations, and the grid's fundamentally an open system and changes in demand can disrupt system operations. So we're interdependent with gas pipelines. An incident on a pipeline could leave a large region without power, so there's a lot of integration into the system that needs to be protected against. We are dependent upon real time visibility and communications. Recent attacks, combined simultaneous attacks on power grid and communications have a cumulative effect. So we just pointed these items out. They're geographically dispersed. We're geographically dispersed, which leaves us vulnerable to a combination of cyberattack and physical attack. The war game statement, you know, if you try and guard everything, you guard nothing. You can't be everywhere at once.

Utility workforce, cybersecurity expertise is limited. That was pointed out in one of the earlier presentations. The resources just aren't there at the moment, and we're dependent

upon purchasing technology that's coming through a global supply chain. I think it's in the news today, Kaspersky being limited in governmental purchases. So the services that are being sold are actually global services and we often don't know exactly what the source of the some of the materials we're using are.

So there are industrial control systems. This was pointed out earlier that we've got infrastructure that's been built up over 50 years, 100 years. It may not have been designed with cybersecurity in mind, and some of that legacy material is still in service. I think the statement was made, I was going to ask about this,

percent interfacing seems to be vulnerable. I'm not sure if I got that number right. I was actually going to ask about it.

So control systems could be used to damage equipment that could take months or years to replace. Buying a substation transformer can have very long lead times. So these are all -- this is just all background information. It's

been pointed out that the responsibility is now split amongst more than 3,200 electric utilities, including entities that may have limited available resources and this gets back to the educational system. How many experts are we producing? I like Hank's approach to trying to create multiple growth of protection that are somewhat independent, but there is an issue in that the commercial entities that are responsible to this protection are not necessarily the ones that will bear the brunt of the damage. There is potentially a dislocation between the costs of an attack and the corporate responsibility for the attack. I'm going to use the Equifax example where, okay, a lot of their information was stolen and certainly they're being damaged, but are they being damaged more than the customers whose information was stolen? So there is a potential disconnect in the value of protection to the company that has control and the potential damages to the society.

Oversight we felt was fragmented.

Regulation of electric utilities divided between FERC and states. So the oversight of security is split between multiple entities. The Fast Act gave DOE responsibility to protect or restore the reliability of the electric system in an emergency, so that is there and it gives DOE at least some leverage into this process. The evolving threats may support placing greater emphasis on the security of the power grid, making sure that DOE's research meets the national cybersecurity need and assessing DOE's partnership model. Is this the proper model for these levels of threat? Those are basically the observations that the Smart Grid Subcommittee made on the multiyear program plan.

I wanted to open up a little discussion on, all right, we've talked about cybersecurity all morning. Do we have any comments on what EAC should be doing, if anything? And I open that up for discussion.

Well, then, I am done. Any questions? Thank you. We're now back on schedule almost.

We've got an update from the DOE on grid security. This is the staff grid study, Travis Fisher, senior advisor to DOE-OE is available to make this presentation. Thank you, Travis.

MR. FISHER: Thanks. I'm putting myself on a stopwatch here. I don't want to extend the overtime.

So thanks for the opportunity. I think upfront I just want to say let's make this interactive because I have a bunch of slides that we could either spend a lot of time on a few slides or just breeze right through and then go straight to questions. So if you have a question, I'll try to see you. Just raise your hand and do the vertical card thing and we'll go that way.

Is there a laser feature with this thing? No? Okay.

So these were the three main bullet points in the April 14th memo from the Secretary to Brian McCormick, the Chief of Staff. These were the areas that we were asked to examine, and I'll be the first to admit each one of these could

be its own staff report and each one of these could take days on its own to do. We attempted to answer all three questions in the 60-day timeframe and it took us twice that long to do it any justice.

So the three areas, these ended up being the three meatiest sections of the staff report. The evolution of wholesale electricity markets, which turned into section five of the report. Compensation for resilience, reliability, sort of the physics of the grid, what does resilience mean, all of that is captured in section four. Premature baseload power plant retirements. That ended up being a very loaded set of words. That ended up being a very large section three to try to address that.

So the process and framework, first, I'd like to note it was an incredibly collaborative effort. There were a lot of DOE staff members that chimed in on the report, and I do want to take some time to note the folks in the room who helped. First of all, the obvious question on

this slide is where is Alison Silverstein? She's an imaginary dotted line. So we brought her on at the suggestion of Bill Parks and that was a great suggestion. I don't think the work would have been possible without Alison, especially given the amount of attention we were receiving from external stakeholders. That was more my role to be the more external facing and Alison was allowed to do sort of the day-to-day work. And I have to admit the group that we put together, you know, I helped assemble it up front and Alison came in and I would say she drove that group like a Cadillac. So it was fun to watch. She was only on for part of the process but her work was incredibly important.

So here we have DOE leadership. National Labs. I'll note we brought in the labs for our May 4th meeting, and afterwards, they said to me, you know, this is one of the first times we've all been brought together for a project like this. And I didn't think I was doing anything out of the ordinary but we ended up getting a

contribution from seven different labs. I'll note especially NREL, Berkeley, Argonne, all of these labs had very good work, and Ryan Wiser and Chuck Goldman in particular. Ryan actually kept at the process and kept bugging us in the way that he does it and, you know, we extended extra rounds of review for Ryan and others, and we were trying to get the lab input. We were trying to get the lab fingerprint in the staff report.

FERC staff also had a round of edits. I'm not sure if that was public knowledge, but they had a small set of experts take a very detailed look at the draft.

Stakeholder input. As you know, we didn't solicit any stakeholder input but we certainly got it and we paid attention to it and we took into account everything we heard in the meetings and everything like that. And the DOE staff portion is the largest for a reason. We had, at the end of the day I counted, over three dozen folks that worked on it. So I'll just note I've been bad at giving people credit so I just

wanted to jot down all the names.

I want to nod to David Meyer, several folks at EIA that I probably can't name all of but I'll name Bill Booth, the whole team at EPSA, and the QER 1.2 process. You know, if we wanted to do something quick, if we wanted to do something worthwhile, we sort of stole some of the processes from what QER 1.2 established. So a lot of the same staff, a lot of the same everything from, you know, citation styles and all of that, it was well, you know, our sort of standard question was how did QER 1.2 do it and let's do it that way. Who am I missing? I already mentioned Bill Parks. He was a big part of this. Larry Mansueti. I saw Larry come in recently. There he is. Thanks, Larry. The whole EERE team, so the SPEA team, the policy folks at EERE. I see Kevin over there. I'll note Steve Capanna, too. And I'm probably going to forget people as I always do, but I just want to say thanks to all the staff that worked on it.

Scope. So we were pretty much allowed

to approach this however we wanted, and some of the feedback with, you know, our conversations with EIA, they, instead of starting at a nice round number like the year 2000, they pushed back and said we don't like the consistency of our data around that time period. We're actually much more comfortable with starting in 2002, and that's the kind of feedback that we wanted to hear. So it was a 15-year snapshot, and that was partly because EIA was much more comfortable with starting in 2002. Still, the 15-year timeframe captures a lot of important events. There's competition. There's the shale revolution. There's the change in electricity demand growth. There's higher variable renewable energy. I'm just going to use VRE from now on out. And we have -- we've seen a little bit of increase in demand response and that's particularly important on the capacity side, and that was on the later end of the time period but it's also important.

This was the trickiest part. When you do this kind of report you have to define things

clearly and it was very difficult to come up with consensus on a few things. We approach baseload in an operational sense and that's, you know, if I had to sum it up it would be the 24/7 plan. Something that can operate around the clock that is controllable. The word "premature" is about as loaded as you get. It's one of those things you kind of -- you know it when you see it and you can take a dozen different approaches and folks have very different ideas on what that means. So if you're a plant operator, if you're in a vertically integrated world that's, you know, you still have some returns that you could get on that plant. If you're a nuclear plant operator, you still have license years but you're not economic. So is it premature if it's before the license term? We introduced all of these different ways of approaching it and said we're not exactly going to take sides on this. They're all valid. I wouldn't argue with any of them. And certainly, in the "you know it when you see it" sense, there's plants like the panda plant where if it's

basically a brand new shiny plant and then it closes within, you know, five years of operation, that would seem to be premature to me but that's still -- it's a judgment that at the staff level we decided not to settle on just one approach.

And these -- I'll go into all these in more detail, so I'm just going to skim over them now. Plant retirements, four key drivers -- gas, low demand, environmental regs, and VRE. And each one of these, you know, we didn't assign a percentage to each in terms of, you know, who had, you know, a specific amount of contribution to it. We did identify gas as the primary driver. On the reliability and resilience end, there is a lot there and I would encourage folks to read -- well, all of the report, but section four goes into great detail on that. And sort of the changes, the way we're going to have to approach things differently in this new world of high VRE, high gas, all of that.

The wholesale markets piece, that was probably my favorite one. That's section five.

That's the, you know, what's going on with the missing money problem. That was identified over a decade ago. Sort of what's the new fun stuff that's going on with that, and we talk about how it's arguably getting worse now and we'll show the supply curves and air cot and all of that. The negative pricing is we bring it up, we raise it, and it's another one of those things, incredibly subjective. If you ask people generally you might not get consensus answers about whether it's a problem or not. If you ask very specific people, if you ask operators of Quad Cities if it's a problem, they're going to say yes. So it's one of those in a blanket sense maybe not an alarming trend; to specific folks, it is a big deal.

And the other thing, the way that states and regions are playing with these markets, it's obviously not just a marginal cost-driven environment. That's sort of the underlying driver in the market setting, but then states do whatever they're going to do between, you know, RPS, X, everything like that. So that's sort of a layer

on top of it that is probably driven by other policy goals that aren't sort of the pure least cost approach. That includes jobs and economic development and national security and things like that.

So I just want to spend a little time on section three of the report. And nobody's stopped me for questions yet; right?

So this, I have to give credit to Alison and Bill Booth and all the folks who had keen enough insights to break the 15-year window into four different parts, and I think that highlights sort of the -- we called the tranches. It's four different time periods that capture different effects. This first time period in the mid-2000s, that's before the gas price drop that we saw. So these are not driven by low gas prices; these are driven by competition in a more pure sense. And if you note, the ownership type is indicated by the shape of the plant, sort of the size of the thing is the size of the plant. A lot of triangles here. A lot of merchant generation. A

lot of pockets in the competition areas where you would expect with CAISO and ERCOT, PJM, New England. As we advance, this is where we start capturing the shale gas effect, the effect of some regs, early regs, especially I would say signals from the federal level that coal is out of style. That sort of MATS versus EPA was a very strong signal against investing in coal.

Now as we go, this I think captures the MATS deadline which was a huge driver, especially in the timing of the closure of a lot of coal plants. So you see a lot of circles here. These are the vertically integrated plants that either closed or switched to gas. And a lot of these are coal but not all. This is actually all fuel types lumped together. And finally, I think if there's a takeaway from 2016 onward it's that no one is safe. I mean, if you talk to folks trying to operate in these markets, it's a tough go. And so I'll just breeze through these quickly again.

Triangles. More triangles. Lots of circles. And now it's everybody. So, and I'll

just note, too, there's just a lot of these. And I think this captures everything above one megawatt, but still, this is a lot of a closures.

This was put together by EPSA, the policy shop within DOE, not the John Shelk shop. Between the two bars, that's the snapshot of the 2002 fleet. And you can see what happened to it. The red is retired. Orange is still operating but announced to be retired. And the light blue is operating with no announced plans to retire. So that just gives you a snapshot of what's going on with the 2002 fleet. And specifically because it's broken up by region, you see that there's a lot going on in CAISO. There's a lot of turnover in CAISO. And at the same time there's a lot of additions as well. So the dark blue is additions. You see some demand response in that paler blue and some planned additions that haven't come on line yet. And it's the same in CAISO. They've retired a lot but they're building a lot. ERCOT is kind of the same thing.

The other thing to note is the total

capacity additions are much higher than the total capacity retirements and I think that has a lot to do with this is nameplate, this isn't prorated for capacity value, but I think if you did prorate for capacity value they would be similar because I think what's happening here is there's a lot of VRE on this right end and higher nameplate capacity, not necessarily the same capacity factor. So I think that's what's happening there. So you'll see actually like fleet average capacity factor is dropping.

If you go by fuel type and by year, it's pretty obvious that 2015, the Mercury and Air Toxin Standards (MATS). The first MATS deadline is a key driver here. I don't think that's going to be a surprise to anyone here. I mean, it's the highest year. It's the highest year ever, and I think that was one of the things that started getting folks' attention in this space is, you know, when you have a peak retirement year, that sort of raises the question of sort of what's going on? Is this worth looking into?

The other thing I'll note here, in the graphic that we stole from QER 1.2 shows net additions. And one thing that gets masked if you look at net additions is if you collapse everything by fuel type though, the closures of gas steam plants are completely overwhelmed by additions of combined cycle gas. But here you'll see there's actually a lot of gas steam that came offline in the 2000s. And that was a surprise to me. You know, folks ask, what did you learn? Were there any surprises? That was the one thing that I was pretty genuinely surprised by. I didn't know the sheer amount of gas steam that came off the grid.

This gets at the other question of, you know, if we're talking about baseload retirements, we're not talking specifically about coal and nuke plants. And in fact, a lot of the coal plants that retired, this is a snapshot of what -- of how the coal plants are operating. The ones that closed in 2014, how they're operating in the years leading up to it. And I'll single out 2013

because I think the blip up in 2014 is just you know you're going to close the plant so you sort of run it without maintenance and sort of run it into the ground. The 13 percent, that's the fleet average for the coal units closing in 2014. That is obviously not a baseload unit if it's running at a 13 percent CF. So that's one thing that we noted. The net retirement figure, there actually was some coal still coming online in the early 2000s, and I think the last one was something like 2014. So the net retirement figure is smaller than the total.

And here's the trends where we see coal on a pretty consistent downtick in terms of capacity factor and gas on an uptick and they actually pass each other. The same with total generation in 2016, which is yet another reason to evaluate these things and say what's going on? There's something interesting here. Coal for the first time was not the top source in 2016 even though I think -- I don't want to do any projections or anything like that, but I think

coal is expected to be the top generation source again in 2017. But the point is there they're actually tied now which is kind of, you know, for the first time ever that's a big deal.

This gets at the other question, you know, what is premature? Is a nuke plant retirement premature for what reason? And I think this is the license point of view. There's a lot of -- so the red X is the plant closure date. The blue bar is the license term. If you add it all, all of the blue bar to the right of the red X's, that's just a lot of potential operating years that we're not going to realize. So that in itself is an interesting thing. The Bloomberg New Energy Finance (BNEF) report saying half the plants are in the red, some folks have said that's an overestimate. I think it's probably spot on, and especially once some of these plants are out of their contracts and have to face, you know, markets again, that's only going to drive more retirements. So this is just one other way to view a premature retirement.

We've already talked about the key drivers. I'm going to go into each one in detail. This I think gets the gas snap shot, and I think the top left is something that everybody knows. I mean, shale gas is incredible. We just have an incredible amount and prices falling. And the thing that I think is a surprising bit and maybe I should have known this, this is something else, there was a lot in the process that was kind of a surprise to me the magnitude of it. I was unaware of just how much more efficient gas plants were becoming in terms of the fleet average. So the fleet average heat rates for gas units you can see that's just more and more efficient in terms of turning a gas BTU into a kilowatt hour. And coal and nukes are very stable. So that only doubles down in terms of the production costs. Not only are fuel costs dropping but the plants are using less fuel to generate a certain amount of kilowatt hours.

The demand piece, again, I think everybody knows this. It's essentially flat since

2005, and we've seen economic activity pick up and haven't seen total quantity demanded. It's not in lock step as it was in the past. And if we have any economics nerds, I'm not talking about a demand curve. I'm talking about total quantity demanded. You can chime in with nerdy questions at any point.

This I think is the more important piece of the demand equation. This is the expectations of future demand. We've been consistently wrong about this and I think that has contributed somewhat to an oversupply based on plants coming online expecting to satisfy a certain amount of demand. That just hasn't shown up. And I'm not picking on EIA. The way they do this is they project current trends outward, and so the annual energy outlook in the early years, that's in orange, pretty consistently above actual. And then, you know, for each year in between it's still every year is above actual. So I think that highlights one of the problems here is that we not only have seen a flattening demand but we have at

every turn expected demand to come back and it just hasn't. And if there's a positive spin on this it's that the DOE is doing its job in terms of energy efficiency standards. But what that means on the power sector side is, you know, we still have in general an oversupply issue based on demand predictions.

Environmental regs piece. I tend to focus on MATS just because that's the biggest driver but we see it across the board. There's just increases in costs, even things at the margin. Sort of the variable costs increase due to compliance. Every little bit counts and I think that's been one of the key drivers in terms of not just shutting down coal plants but increasing their operating costs. And you see that of the retired and switched to gas there is actually quite a bit. And in the no change category there were a lot of states and regions that required the same kind of equipment, so in terms of the compliance piece there's only a small piece.

This again, this isn't news to anyone, but with VRE rising and sort of the -- so all the text is really small, so the orange piece is wind and the yellow piece is solar. And the large chunk being hydro, then biomass and geothermal. Those three have stayed relatively flat throughout. They're certainly not growing. And then wind has seen incredible growth and solar is on the cusp of the same kind of incredible growth. And I think the, you know, there's two different ways to see it. There's the looking backward at existing data, so the LBNL chart here, that is maybe not the most intuitive way to do it, but the gist is if you're going to try to plot a line on that -- I don't know if there's a line that fits on that. And the outlier obviously is -- we've seen a lot of retirements in VRE and CAISO, but in general we haven't seen the kind of correlation that you might expect. I do expect this to probably change in the future but, you know, we have to go with the data and they don't indicate a correlation.

So this gets to section four of the report. And this is where we leaned extensively on NERC. You know, we're not trying to --

MS. JEREZA: Sorry, we have a question.

CHAIRMAN ADAMS: This gets into -- you have the reliability adder in ERCOT and maybe you're about to get into that, which is a little bit different approach than anything - - anywhere else -- I think anywhere else anywhere. And we don't have a capacity market and there's certainly a different capacity value of VRE resources, I think. I think, that's opinion, than of a traditional just fuel-based resource. And I admit, I've read a little bit of the report; I have not read all of it. Do you discuss anywhere the --

MR. FISHER: First of all, I expected everybody to read all 187 pages and I am very disappointed. Go on.

CHAIRMAN ADAMS: I am, too. Do you discuss those approaches anywhere? Was that in the scope of this report at all, the different --

the market approaches versus capacity market approaches versus reliability adders? Is that in scope? Can you discuss it at all?

MR. FISHER: You're teeing me up for sections four and five that I'm going to get into. So this is perfect. Thank you.

So the capacity value question is huge and that's captured in section four, and that's more of an engineering calculation, and section five is the next thing we'll go into which is the markets piece which I will never say anything bad about ERCOT. I think they're doing it right. I think in this report we don't take a side on capacity markets versus not. Each region is going to have its own approach to that. Yeah. You teed that up. It's a few slides away.

CHAIRMAN ADAMS: Oh, I got what I wanted. Thank you.

MR. FISHER: So we do have to change the approach somewhat based on changes we have seen on the ground. The idea that the portfolio is changing, that in itself isn't necessarily a

problem. In this section we tend to key on the existing NERC reports and also stuff from PJM and other RTOs. And we don't see a reliability issue with sort of high gas penetration, high VRE. I think that does raise new resilience questions. I think those are worth addressing, and that's sort of where the attention is now on the margin. And the other thing to point out is -- and this is yet a further section. This is the affordability section, section six, which is very thin. It gets to the question of if we're -- if markets are set up to give us a least cost very efficient answer, you know, from a policy point of view we have to ask if that's giving us all the other things that we also want. So is that giving us a reliable grid? I think it is just based on the work that utilities and FERC and NERC are already doing. Open question as to whether the new resource mix from the generation side is also resilient. So that's sort of the new approach.

I should have noted we got two very good notes from -- one from NERC and one from PJM and

they were on the same day on May 9th, and they essentially said we noticed you're working on this thing. Here's what we'd like to focus on. And it's the stuff you might expect -- ERS, flexibility, fuel security, new transmission. And I think that gets back to the previous slide about, you know, if we want to build a system that's reliable, resilient, and has all these other characteristics, like fuel security, those things tend to come at a cost. And so it's important to note that, you know, if we want an affordable grid it may not be exactly the same as a resilient grid. And there's some tradeoff between those two.

MR. KEZUNOVIC: I have a question. So when you were talking to NERC, is this the definition of what reliability and resiliency is that you have adopted? Because, you know, we have flexibility, adequacy. We have many things to look at for reliability and resiliency. But there are things that are not in this to look at.

MR. FISHER: Oh, yeah. So --

MR. KEZUNOVIC: So in answering the question that was posed originally by the memo, were you directed in any way how to define reliability and resiliency before you would try to give an answer or --

MR. FISHER: No, we didn't get direction on the definitions, and in fact, we borrowed NERC's definition of reliability, and NERC itself borrows -- I forget who it is but they, in fact, don't use their own resilience terms. So that's -- it's been interesting to try to define those terms. And I guess one thing that I'll point out that we get into this later is, you know, I've gotten the question a lot, what's the difference between reliability and resilience? And it is defined in SERC terms in the report and I don't recall the exact wording but I think the fundamental difference is you can have a very reliable grid that is not resilient. You can have in sort of the abstract -- if you had a 100 percent gas grid that was fueled by, you know, non-firm contracts, by single pipelines, that

would be in sort of the day-to-day operations, that would be a reliable system but it wouldn't be resilient to a polar vortex type event.

MR. KEZUNOVIC: Yeah, what I was referring to is, you know, there are different sizes of this as you said. And in order to give an answer one has to kind of put the reference out there so that one knows what one talks about. And I'll just reflect on one aspect of this that I don't see necessarily here but the infrastructure itself in the United States is on average pretty old. Those are the assets infrastructure. And the value ranges from 850 billion to a trillion or whatever it is. So it's one issue there that the assets may contribute to the resilience and reliability.

So some of these views here may or may not relate entirely to the issue of the assets even though the generation resources and things like that are part of the picture. But the grid itself, the wires and the iron and stuff like that is another component which leads into reliability

and maintenance and other things. So I'm just trying to get an understanding how much of this complex issue have you grasped so that one can understand how compulsive the answer is?

MR. FISHER: So we can take a deep dive on this. I think the way to define reliability, you already split it into two different parts. There's the operational piece and then there's the resource adequacy piece. So I think in both cases we are doing very well and the term that NERC uses is the word adequate. So we have adequate resources and in operational terms we have all the things that we need currently. So that's the sort of two-part approach to the reliability question.

The resilience question, I think the fact that we don't have very clear answers on how to define that, that's exactly why we care about this space because I think it is important for, especially at the RTO and FERC level, to start trying to wrap our minds around exactly what we mean. And --

MR. KEZUNOVIC: In the interest of time

I'll ask one more question and I'll kind of let it go. I'll read the report if I need to understand more. But have you looked at the outages in the grid? Are the outages in the United States in the last decade, 10, 15, 20 years, are they going up in time and frequency? Or are they going down?

MR. FISHER: Well, then we have to take yet another slightly deep dive. When we talk about the grid, I think the only major outages on the bulk powers system that we've seen, you know, as you know, between Alison and David we have the authors of the 2004 report reflecting on what happened in 2003. That was clearly a major outage at the bulk power system level. Most of the outages that we focus on are actually on the distribution level. So that was not necessarily beyond the scope of this report. We just don't spend time on it because we have to draw scope lines somewhere. And so I think the bigger question -- I think in both cases we're doing very well. I don't think there's a trend upward in either but I'm not sure. We didn't look at the

distribution level outages for purposes of this report, and all of the bulk level outages are obviously very well known. And also very infrequent for a reason. So in terms of the trends, I think your question is more on the distribution level and we didn't take a deep dive on that.

MS. ABDEL-KARIM: So I work with NERC --

MS. JEREZA: I'm sorry; we have to prioritize the comments and questions from the Committee first and then we'll have public opportunity afterwards.

MS. ABDEL-KARIM: All right. I'll maybe follow up later on the NERC piece.

CHAIRMAN ADAMS: So we need to get you to sign up for public comments as well. Thank you.

MS. ABDEL-KARIM: Thanks.

MR. FISHER: I will note -- so I don't want to respond out of line but I will just say there's info in the slides from something that she authored, so I just want to point that out.

As you go, this is also a NERC diagram. I think this gets at the flexibility piece and it tees up the economic piece that I'll get into in a second, is if you just compare the load curve on the top, which is the original that's just demand by itself, the load curve without any netting of VRE, that's a relatively smooth curve. The dotted line, you're already sort of moving away from that and changing the shape of it. That's with wind, and I can't remember the amount of wind penetration that that assumes. Changes the curve but only slightly. I think the more interesting effects happen with an increase in solar. So everybody knows about the duck curve, et cetera. This is somewhat the same where the shift in the peak, of course it goes later in the day. This is net load, so this is load net of wind and solar. So as you increase solar, you're not decreasing the net peak load as much as you go and that's indicated by the colored lines.

And the other thing to note here is just if you compare the blue line to the black one at

the top, the black one is relatively smoother and the blue one is a little more jagged and you can see why we're talking about the flexibility of the system. You need to meet sort of a shakier net load.

And we're stealing more from NERC here. This is the resource adequacy piece on the left, and that's sort of a -- you need to get an accurate picture of capacity value if you're doing resource adequacy analysis. And then the thing on the right is, what is the capacity value of solar as you get more and more of it? And you can see it drops off pretty significantly. And I think that's an important piece. And I believe we stole that from NOAA's piece. So thank you.

But even at the five percent level which we're already seeing in CAISO, the capacity value of new solar is, I mean, it's fallen from 40 percent to eight percent. So that needs to be taken into account and that sort of changes the analysis of how do we think about new capacity? How do we think about resource adequacy? And I'll

note there's other changes on the other end where maybe we don't have to think about capacity in the same way if we also have demand response. So if demand itself is flexible that also changes the equation. So there's a whole bunch of new, interesting stuff in this space.

On this one we lean on PJM and I'm sure every RTO has their own take on this. The PJM take we thought was important. This is from a March 2017 report. And we highlighted the red boxes. We just wanted to highlight how the attributes can complement each other. So if you compare nuclear to solar -- sorry, to storage, they actually have very -- I would say they're very complementary in terms of the attributes that they bring. So there's a column that talk about ERS, fuel assurance, and the text is kind of small. It goes ERS, fuel assurance, flexibility, and other. And for example, if you focus on rep capability or flexibility, storage has everything you need, nuclear doesn't have anything. But the thing that nuclear does bring to the table,

obviously, if you key on the fuel assurance column, nuclear does very well and storage doesn't.

So I think that gets to the idea that we don't just need a diverse grid; we need to be smart about the kinds of pairings that we have. And this actually indicates to me, I mean, the idea that you would pair a nuclear plant with a pump storage facility that kind of goes hand in hand, you can see why those are -- they just go very well together.

And as the fuel mixes change, so we're -- obviously, our focus in terms of reliability and resilience has been on the generation side and we get a lot of questions about why was the focus so much on the generation piece. I think it's just because it's the new shiny object. It's the thing that's changing the most, and I think that merits the amount of attention that we've given it. And as you can see, we do a snapshot. This is national level. Each region is very different. And we actually do -- EIA gave us a regional

breakdown. Each of the nine regions that we split the U.S. into we go into great detail on things like this. And that's in Appendix A of the report. But this is a national level thing. In 2002, 09-16, you can see it changing. So all of the blue is some type of gas. So it's pretty obvious that we're getting into a more gas-heavy grid.

The other interesting thing is if you just look at the generation share, nuke has stayed constant at 20 in that timeframe.

And the one key takeaway is the focus shouldn't be on diversity per se. It should be on what diversity gives you. So if we want reliability or resilience, we should focus on those things themselves instead of the abstract idea of are we diverse. Because we certainly are more diverse now than we have been in the past.

MR. KEZUNOVIC: Quick question. Was there any discussion about whether the centralized generation versus distributed generation has a role in this?

MR. FISHER: We didn't get into distributed that much. I think when you go down that route it ends up being in practice mostly solar PV. And I think that if anything, we could go back to the PJM piece where solar obviously brings a lot of attributes and that's the way I would answer that question. We didn't parse distributed versus not in terms of their characteristics.

And in terms of just answering the question, what was the difference between reliability and resilience, I think PJM answered that question pretty well in that March report when they said we took 98 hypothetical portfolios. And they were all considered in terms of reliability, they were all considered desirable. What happens when we subject all of those 98 portfolios against a simulated polar vortex type event? You lose two-thirds of them. There's only one-third that ends up resilient to that kind of test. And I think that's an important test that each region is obviously going to have a very

different test that they need to do. It makes sense for PJM to do a polar vortex type test and as we go through, if you're a gas-heavy region, it makes sense to focus on sort of the gas interdependence with the grid and storage concerns, new pipeline concerns. For our part, you know, we encourage new builds of both transmission wires and gas pipelines, and that's always going to be part of the answer.

The extreme event question. So for Northeast and PJM, it makes sense to test against a polar vortex type event. A lot of these things are very hard to predict, obviously. The polar vortex, nobody saw that coming. Super Storm Sandy, very hard to predict. Hurricanes are perhaps easier to predict and more common. At the same time, who knew that we were going to get with two back to back after 10 years of just not seeing any? So now the folks in Florida, the outages, a third of customers don't have power. And again, that's on the distribution level for the most part, and I think the interesting there, and this

is a sad note, I saw in the paper this morning that there was a nursing home with a generator outage and some folks died because they couldn't get the AC running. And if anything, it just highlights the importance of, you know, what utilities bring to everyday life. I mean, that's obviously the kind of thing that we would very much like to avoid in the future.

So this is my favorite part, the wholesale markets part. And I have a FERC background so this actually does get me excited which is, I know, that's weird.

So this I think addresses the question of what's happening with energy versus capacity and how you address the missing money problem and things like that. A lot of regions have gone the capacity route, and if you talk to Joe Baring at PJM he's going to say, look, we expect as low marginal cost units, low fuel cost units are increasing so you know, gas and VRE and PJM, this green section, the energy price, the energy revenue to a plant, that's going to shrink and the

capacity piece is going to grow and that's his answer to it. I think the remarkable thing to me is that people don't have -- you talk to experts, people who have lived this and they don't have consensus over what the right structure might be. And obviously there's an ERCOT structure which includes, you know, you take away price caps and you sort of use an energy price only with the operating reserve demand curve. And there's a bunch of different answers to this question but this is the question and it is changing because we're seeing an increase in VRE and a lowering of fuel prices. And this is what it looks like. This was amazing to me, and Alison just left, but this was kind of her idea with Bill Booth and it was just a question of if you build a dispatch curve, what happens with just changes in the fuel prices? So these are actual fuel prices and actual units in ERCOT. And I'm not saying they're all available all the time but this is the hypothetical dispatch curve that you would get if they were all available.

And this is pretty amazing. I mean, I'm a more visual person so this stood out to me as, look, in 2005 with the gas prices we had then, you get a very steep curve. You can see how you would get a price spoke in the demand range of gigs. You would be getting sort of the $80 price range. And I think that's amazing, especially when you compare it to in 2011 in that same range you're looking at prices in the $30s. And again, falling even more in 2015, those prices are around $20. So that's the -- that's sort of a summary of what's been going on with fuel prices.

And I think the other thing to note, if fuel prices ever went back, if you ever had sort of the lack of shale resources, we would have a supply curve again that looks more like 2005. And while that might be good on the producer end, I'm not sure that that's what we'd want to see. And also, in 2015, the thing to note, especially compared to 2011, so the coal section of the curve is all by itself, one notch lower than even cc gas in 2011. And then in 2015, it's exactly mixed.

So you have gas being dispatched before coal and things like that. So that's just -- I think this captures a lot and this is sort of just a visual snapshot of what was going on with the fuel cost changes.

And it also indicates that if you're relying on price spikes to drive your missing money solution, in the absence of transmission constraints, you're just not really going to get them. And the ERCOT folk will tell me there are plenty of transmission constraints. So that's -- some folks are very comfortable with the way it's set up even with this very flat supply curve.

We address negative pricing only briefly. Again, it's kind of -- when you take a broad view, there's no reason to panic. If you talk to very specific pockets, if you say, you know, if you're on a nuclear bus, again, if you're Quad Cities, it's a very acute problem for some areas, and system wide, I'll note the Hogan-Pope paper on ERCOT saying there is a price suppressive effect and the presence of the PTC does

incentivize when to sort of power through the negative pricing events. But in general, I mean, in the LBNL sense, two percent of total hours in real-time markets in 2016.

This is the piece that we didn't dive into as much as I'd like, and I think it's just a product of there isn't as much out there as I was expecting. We do want to answer questions about affordability. We want to be able to say, you know, what is sort of a bulk power system that's affordable? What does that look like? We don't even necessarily have good metrics for it. If you just look at LNP, obviously, it attracts gas and in the higher gas price world, in the early part of the 2000s up to 2008, you have wholesale prices on one set of normal within a range and then post-shale boom you have wholesale prices on a new lower normal. I think the puzzling thing for me is if you have, you know, starting around 2010, very low whole sale prices, what's taking so long for that to be reflected in retail prices? Is it just a very long lag or is there something

structural that's preventing it? Or is it just 100 percent compensation from the costs that you're lowering on the generation side? Are they being made up -- are the costs increasing that much on the transmission side, for example? But that's all going on on the bulk power system. And then, you know, even if you're just looking at generation and transmission and not the distribution load- serving piece of it, we don't have a good snapshot of how to talk about that affordability. You know, it might be something like a system-wide LCOE that takes into account cost of generation plus transmission, and we just haven't really seen a very good metric for that. And the blue bars are just, you know, resale price changes. You know, if wholesale prices were going up, this would be a very positive thing that you don't really see them reflected in resale price increases. You also don't really see retail price decreases with wholesale prices either.

And finally, if you were in the media meeting that we had the day we published the

report, this was the section that you flipped right to. Section seven is policy recs. This is one where, for the most part, for DOE's piece, we're going to keep going. We're going to do the things that we've always been doing, shifting focus. We're going to prioritize things, sort of the regulatory reform angle, executing the EOs, things like that.

One very recent example, I think it was Tuesday morning, we announced some awards from the Office of Electricity. And I can't speak to the specifics of those, but it was a $50 million total -- potential total I should say. Sorry, Katie. And obviously, some go outside the scope of DOE. And again, this was a staff report to the Secretary. It wasn't a DOE official stamp of approval on all of these policies. But we do look to FERC to speed up what they are doing on energy price formation, sort of the valuation of new ERS to sort of tweak the way they've approached that. And again, in most cases it's not something brand new. It's just we've been talking about these

problems for years and I think it's a fair question to ask now. What's the hold up? Let's get moving.

And some look to EPA. There's, you know, even on the gas side it says allow coal-fired power plants to improve efficiency. There are regs that affect the existing fleet and it's not just the coal side; it's also the gas side. And we think especially if they are environmental regs, it's backwards that an environmental reg would have negative environmental consequences. So that is, again, we thought a more obvious sort of policy rec. And the Office of Nuclear Energy wanted to talk about revisiting NRC regs and I think that is important, certainly important to them. That's not my expertise so I can't really speak to those.

Further research areas. This, I think it is more where there's a pivot. What are we paying attention to? What kinds of things are we studying? I think if there's a change in focus, it's partly to move away from a designed

transition. You know, there's the -- just in the title of QER 1.2 it was transforming. With sort of the implication being that it was the DOE that was going to be do the transforming. I think with a market-based approach it's more of a allow the transforming, monitor the transforming, try to figure out if the transformation is what we want and what we need in terms of reliability, resilience, et cetera. And especially, I'm going to keep going back to the cost and affordability question. We don't have very good answers for, you know, what things cost or what a low-cost portfolio would be, what a least-cost portfolio would be. And what that would give you on a baseline is if you want to move away from that, if you wanted to guarantee, for example, that the existing nuclear fleet stayed on for longer, that would allow you to put a price tag on those policies. I don't think we have a very good concept of the cost of doing certain policies. And from the point of view of a staff report, or if my job as an advisor is to advise policy, when

those policy questions come up it would be nice to say you can go that route if you go that route in sort of the if-then statement. If you go that route, then it will cost X. But we don't have a very good concept of that. And we expect to keep an open dialogue with FERC.

You know, just as an anecdote, when I was getting briefed about all the different DOE programs, the thing that stood out to me was I saw some overlap based on my experience at FERC and then hearing about what DOE is doing. And I would ask, I mean, at some point I was kind of tired of asking, you know, well, do you talk to FERC about this? Is this the kind of thing that you meet with FERC? I mean, how much interaction is there? And the answer 99 percent of the time was none. We don't interact. We don't talk to them. And the answer was they're an independent agency. Yes, they're independent but that doesn't mean we can't talk to them. So I'm going to try to keep those lines more open than they have been in the past.

And again, 187 pages. But at the same time, I encourage you to read the whole thing. And if you have input on a voluntary basis -- we're not soliciting input, but if you have input, we have a site set up for that. And these are hyperlinks if you go to this on the EAC page. And I'm just going to open it up to questions.

CHAIRMAN ADAMS: Any questions or comments? Jeff?

MR. MORRIS: Thank you. There was an earlier question about, you know, looking at the distribution system, and part of what I'm concerned about when you get a lot of input from some of the system operators is that there's a competing view of thought out there in the policy world that, you know, the change in the business model at the distribution service level and going away from volumetric sales. So when you start seeing a fully integrated DER process where, you know, community solar is being matched with EV charging stations and park-and-rides are shared, commercial solar because the commercial rate class

is one that with their peak and so forth during the day. You're seeing the levelized cost on a 15-year shared commercial solar be cheaper than what the rates are for the sticks and wires.

I've got some cooperatives out in my neck of the woods that 92 percent of the cost that they charge their customers are the sticks and wires, and eight percent is the cost of electricity. Now, we have cheap electricity in the Northwest, but the people that service them on a customer basis are saying, hey at some point we may have to supply a farm managing management system with propane generation and PV as a service and not have them connected to a distribution system anymore.

Where I'm going with all this is that the erosion that's going to happen in the business model at the distribution level is going to cause, I think, a cascading failure up to the high voltage system when you start seeing that amount of demand drop off. So it's almost the opposite view I think of what you got from the NERC

perspective. And I just think it's a mistake not to take that, you know, devolving business volumetric business model into account when we're looking at this.

And I think the other comment, too, is that if you look at the amount of retirements in state-regulated portfolios for regulated utilities around 2030, that's going to be a huge kind of watershed range where all those third generation coal plants are scheduled to be decommissioned. They can still operate but obviously, that's where they are booked out to be decommissioned at some time, that 2030 to 2035 range. You know, I think that's from the state policy perspective. We're having lots of discussions. Okay, what's going to happen with the high voltage system at that point? Are we going to have the same discussion we're starting to have with the distribution system where all the activity is going to be there and there's not going to be as much in the interface, which is what the paper that's being written on the transmission distribution interface by one of

the Subcommittees I think is just critically important to start looking how that relationship is going to evolve. So I guess it's just more of a comment that there's, you know, if you talk to folks on the distribution side, I think you might get a different picture. You know, the customers are going to be driving these changes as much. And once you see that distribution model move away from volumetric, then the high voltage system is not going to be able to be supported by a volumetric one.

MR. FISHER: Yeah, I agree with that completely. And we certainly got that perspective from the California folks. That's sort of the extreme end of the current set of examples that you can study. I think the important thing where you and I would certainly overlap, which is the idea that if we're in this very dynamic space and we're not sure exactly how things are going to shape up, it makes even more sense to go on a more fundamental level in terms of pricing and getting prices right instead of all the things that in the

past had been bundled. You know, you have your ERS and energy itself and the way you approach even the capacity value of a power plant, all of that analysis in the past was relatively straightforward. And now it's getting more complicated but I think it's worth looking into parsing all of that out so that we can be, you know, we talk a lot about being resilient to weather events and attacks and things like that. I think the regulatory structure itself should be more resilient to those kinds of changes. They should reflect, for example, the pricing should reflect if things fundamentally change, if fuel prices fundamentally change. If we have a lot of increase in things like net metering, et cetera, we should be able to not just have to react to that on a process that takes five years. We should set it up now and figure out a way to be resilient to a handful of changes that we could foresee or even not foresee. So it gets to the regulatory environment and the lag that we're seeing and sort of the bogged down nature of a lot

of the stakeholder processes and how long everything takes. I think if we're still stuck in this reactive environment a few years from now, I think it's going to be very difficult to react quickly enough to capture all these changes. I think there's going to be a lot of economic efficiency lost if we don't react quicker.

CHAIRMAN ADAMS: Any other questions or comments or discussion of that last issue? I'm wondering what should we be doing now, I guess I want to ask that, to make ourselves more resilient?

MR. FISHER: So I think specifically, you know, the staff report tees up a lot of issues. I think almost every -- every time you talk about what you might specifically do, I think that's a policy call. I think it's just a matter of, you know, what's the standard you want to meet? What is of the most importance? You know, like Hank said, you can't be everywhere at all times, so you have to prioritize something over another. And ultimately, that's a policy call.

So what we were trying to do with the staff report was arm Secretary Perry with the best information on sort of the state of things and, you know, if his policy answer is, you know, we need to keep existing nuclear plants around, that's sort of like one example that gets thrown around, you know, ultimately, it's up to him to make that policy call but the answer to that question, sort of what should we be doing now, I think that rests with the policy folks at FERC and at DOE and at others. And at the state level, too.

CHAIRMAN ADAMS: Okay. Thank you, Travis. We're running a little behind, so I want to move us on to our Subcommittee reports.

Laney, I believe you're up first with Smart Grid.

MS. BROWN: Yep. Thank you. Just to provide a little bit of background for new Committee members, in terms of the origin or the -- maybe not -- the basis of the Subcommittee itself, it does have a statutory basis coming from the EISA. And in terms of our role to advise the

DOE, it's focused on the development of smart grid technologies that transition to applied use of the smart grid technologies, as well as development of technical standards in areas such as interoperability and intercommunication. And then also, the optimum use of federal funds basically to encourage such progress. And so that is, as we go about our business in terms of the Subcommittee, that is, you know, we need to keep in mind.

In terms of what we have been focused on over the course of the last nine months, we have, I think as you heard today, and actually, a culmination of a lot of the work today comes from the Smart Grid Subcommittee, obviously, the focus around cybersecurity. I had previously mentioned and referenced the Internet of Things panel, whether it relates both to the elements around the development of smart grid technologies interconnection and grid edge, but also from a Subcommittee perspective, meeting on the discussion of the cybersecurity issues as it

relates to the IOT and power grid.

We heard a little bit today from Hank, obviously around the multiyear plan from a cybersecurity perspective. So I think you heard a lot of that discussion. Carol had also talked about new trends around grid edge and IOT. Some of the examples that Hank had presented around industry-led initiatives that were discussed on that call, and really, I think that from that perspective the discussion and focus has led to what you've realized or seen today. Feedback on that multiyear plan for the energy sector, cybersecurity. John presented out on our feedback from that as well as the panel that we presented today. And I think then, you know, queuing up really and I think John had maybe done some recruiting. I will also say we're definitely looking for Subcommittee members. But the areas that we are looking to further consider and develop are around cybersecurity and Internet of Things. So evaluating some of the information that we heard today from the panel. And

additional, maybe building off of the feedback that was provided for the MYP work, as well as looking at considerations around infrastructure investment in the grid.

I will just say that these are concepts, and I think we are absolutely interested in folks' input in developing further ideas. Either these ideas further or additional areas. So definitely an opportunity for Subcommittee Members, or new Subcommittee Members, to provide input onto the developments going forward for the Subcommittee.

Any questions? Thanks.

CHAIRMAN ADAMS: The next report is on Power Delivery which I will deliver. I need help in getting my -- ah, there we go. I am fortunate in leading the Power Delivery Subcommittee that does not have statutory obligations to deliver products. So what we're working on at the moment is a look at the transmission distribution interface with increasing amounts of distributed energy resources. Heather Sanders, who could not make it today, is leading that effort, so I get to

stand up here and take credit for her work. With the help of ICF and DOE, we created a list of the documentation of DOE activities in this space and they've actually done quite a bit. One of the reasons I haven't read the last report is I'm still trying to get through the other reports on this particular issue.

Our intent is to try and examine the differing conditions across mostly the United States, different regulatory and physical paradigms. Turns out that ERCOT is not exactly like California, and neither one of us is exactly like PJM or Southern Company. So what we've done is we've generated a list of proposed topics -- oh, I'm sorry, a lists of regions and selected interviews -- interviewees from each region. What we did is we went to people from different parts of the country that knew people in those regions and asked them to propose people we could interview on this topic, experts in their particular area. I provided a couple from ERCOT. We got some from California, the West, from the

Midwest, from the organized markets over on the East Coast, and then from what I'm calling the non-organized, the more traditional utility structures. And finally, we had some international. And we selected interviewees from each of these regions and have been going through a process of phone interviews, the intent being to examine the differing conditions across the different regulatory and physical paradigms and consider the DOE activities in light of these different regional differences.

So we've done three interviews. So far, boy, each one of those regions had two, so I guess I can do the -- two, four, six, eight, 10, 12. We've got 12. So we're three- twelfths done. Got Heather's leadership on that, and I'm carefully not saying we'll have a product in February, although we'd like to.

We're also working to define our next Work Product. I had a list of six things for us to look at. I was hoping that we would close it and select one. We had a meeting yesterday before

this meeting began. It was unsuccessful. Successfully crossed off of those six, crossed off four, and I've since had, because of our discussions over the last two days, I've added one. So two steps forward, one step back is where we're at. Anxious to get new Membership onto the Committee, so I'm continuing to recruit for all the Committees. If you have not signed up for a Subcommittee, please do so. And we preferred to defer making that final selection until we had new members signed up.

So are there any questions? Boy, we're just powering through. Thank you. And now Ramteen will address the Storage Subcommittee.

MR. SIOSHANSI: All right. So I'm Ramteen Sioshansi, the new Chair of the Energy Storage Subcommittee. And I'm just going to go really briefly through.

We currently have four Work Products in various stages of development, and so I'm basically just going to give a quick background and sort of what the status and next steps are for

each of these four.

So to start with we have this Work Product on energy storage for resilience and reliability. And the basic premise here is that there's a recognition that storage has a potential role to play in improving or, yeah, in addressing resiliency or reliability needs of electricity service, at the same time also serving sort of the system's more routine needs. And so the purpose of the Work Product is sort of to survey the sort of potential use case where you're on a day-to-day basis using storage for addressing day-to-day grid needs but also having this resource available to help with resilience and reliability issues.

The Work Product actually is building off of a day- long workshop that was held in the June 2017 EAC meeting for folks who were here back in June. So we suffered a temporary setback with this which was that the three primary people who were working on this Work Product -- Janice Lin, Ake, and Laney Brown -- two have come off the EAC

since the June meeting. However, I've confirmed as of yesterday or last night that both Ake and Janice have volunteered to continue providing their time and effort in getting this Work Product completed. And Laney has also volunteered to basically be the lead EAC Member in developing the Product.

So basically, in terms of progress and next steps, workshop material, transcripts, and notes from the June 2017 meeting have been compiled, and basically Laney is leading drafting of the Work Product for team review, meaning the broader Subcommittee. And the hope is to have the Work Product ready -- this is not a typo -- for the February 2018 EAC meeting. So we're keeping our fingers crossed that that progresses along that timeline.

Second Work Product has to do with alternate storage technologies. So this was also a Work Product proposed originally by Ake, but Jim Lazar has taken the reins on it. As a little bit of background, Subcommittee Members felt as though

the EAC has sort of historically focused on electricity and electricity out storage, and so the purpose of this Work Product is mainly to be a relatively brief definitional and scoping document on alternative storage technologies that don't sort of fit that electricity-in electricity-out characteristic. So it's going to be very limited in scope. The idea is that we would later have follow-on work products that would provide more concrete recommendations to the Department, identify opportunities, challenges, so on and so forth for the Department to pursue.

So at this point in terms of the progress made and next steps, Jim has put together a scoping memo that basically highlights alternate storage technologies. You circulated that amongst the Energy Storage Subcommittee. I know that a few people have given him feedback and he's in the process of revising that. And then we're also having discussions within the Energy Storage Subcommittee as to if there are other technologies or other things that we want to address in this

limited Work Product or if we're happy with the scope that we've identified so far.

Next, we have a Work Product looking at rate tariff regulatory market design for energy storage. This was actually proposed by Tom Sloane, who is a former EAC Member, and I have taken the lead on getting this -- pushing this product through. So the basic premise is that sort of the traditional regulatory approach that treats assets as being either market-based or rate-based for cost recovery and other purposes may not be suitable for energy storage that can potentially cross these boundaries. And so what we're aiming to do in this Work Product is basically raise some of the issues that energy storage may face from a regulatory market design perspective. Try and survey what has been done. So what has happened at the state and federal level and in different RTO and ISO markets and what have different utilities done to try and address these issues. So sort of to raise a lot of questions, survey a little bit of what's been

done, and then leave recommendations to the Department as to, you know, what it can do to help facilitate addressing these issues going forward.

So, so far we do have a working group. We've drafted a starting list of sort of topics and issues that should be raised or pertinent in the Work Product. I think at this point we need to probably pare that back a little bit because I think we've sort of -- we put everything and the kitchen sink on that list and we're running the risk that this Work Product may take 20 or 30 years to write, which is a little bit longer than I want to wait. We're also trying to schedule a conversation with some people in DOE to see how the list should be refined or expanded so that we actually provide a Work Product that's useful to them and that should be happening shortly after following this week.

Final Work Product. So we have a 2018 Biennial Storage Review. This is one of the few EAC Work Products that actually does have a statutory requirement. So I've excerpted two

subsections of the EISA and the one that is highlighted in red is the one that applies to this Work Product. So basically, the Energy Storage Subcommittee every five years is supposed to develop sort of a forward-looking plan for how the Department should address energy storage, research development, and deployment, and then every two years we're supposed to do more of a, I'd say, backward looking, how has the Department been performing in addressing, you know, the goals that were established at the last five-year period.

Incidentally, a quirk of math, five and two are not divisible by one another so there are occasions that you end up doing three of these Work Products three years in a row. We actually decided in the 2016 Work Product to combine the two- and five-year requirements so that we didn't have to do the five-year goal-setting document this year. So we actually turned in our homework a year early which is always nice.

So as far as this Work Product is concerned, the progress so far is none and that's

intentional. That's in large part because we have not gotten a response from DOE to the 2016 review document that we provided them at the end of 2016. My opinion is I would personally rather wait if we can to get a response to that so that, you know, we're sort of on the same page before we begin working on the 2016 review. My understanding is that hopefully a response should be coming fairly soon.

Now, ultimately, I would say that by probably November of this year at the latest, regardless of whether we have that response from DOE, we really do need to begin working on this Product and that's just because the 2016 assessment really did take about a year to get it all buttoned up and everything. Thank you to people who have scheduled next year's meetings. We actually have an extra month because instead of a September 2018 meeting, we have an October 2018 meeting. So we can reasonably wait until November to start on this and be able to get the Work Product hopefully ready for a formal vote and

approval in that October 2018 meeting.

That finishes it. Any questions? Comments? Or agreement?

CHAIRMAN ADAMS: Ramteen, I've just got one. You've got a lot of parallel Work Products going on. Is it reasonable for you to consider, and you don't need to answer this, turning one of those into -- deferring one into a later time period?

MR. SIOSHANSI: It's certainly an option that I've kicked around in my head at a few points. I'm of the opinion that I think we can get these Work Products finished. I realize that it is a fair amount and we're relying on people to volunteer their time. So clearly, the fourth one we can't because that, you know, we want to get -- we want to provide DOE with what we're supposed to by the end of next year. And the first two I am -- I don't want to speak too much for you, Laney, but I feel like the first two -- well, the first one you've told me that early next year is when you're targeting for that to be complete, and then

the second Work Product, again, I think because we've identified a relatively limited scope for it, I'm also hopeful that that's not going to be a huge investment of time. So the only question becomes the third Work Product. I'm of the opinion that it's a very important issue so deferring it for a few years is probably just going to be detrimental to the industry as a whole.

MS. BROWN: Yeah, I was just going to comment. I think they're at different stages which allows the completion to be done. Even though they seem like they're happening simultaneously, because they're at different stages, so I think it's --

MR. SIOSHANSI: That's certainly very true. So the first two Work Products are much further down the pipeline. The fourth one, nothing has happened. And the third one is very much in the preliminary stage.

CHAIRMAN ADAMS: Thank you. Are there any other questions from the Committee?

We have arrived at our public comment portion of the meeting, and we actually have two people signed up. Theresa Pugh, are you available? You have the podium for five minutes.

MS. PUGH: Thank you for allowing me to speak. I don't need the full five minutes.

I'm Theresa Pugh with Theresa Pugh Consulting. I come from the electric utility industry and have some background in oil and gas, including pipelines.

I wanted to encourage at future meetings that you might look at some localized infrastructure issues that might have localized and not grid impacts, but might be significant enough that merit some additional discussion by your group or contractors to your group on other types of solutions, such as the possibility of using LNG and other forms of gas storage across the country in states where the geology is ill-suited for natural gas storage in those particular states. I wish every state, Mr. Chairman, was like my home state of Texas, and

yours. You know, it's a bowl of spaghetti of a wide variety of product pipelines under the ground that have served the oil and gas industry and the electric industry beautifully. And I hope that works in every state. But there are going to be some transition issues in natural gas -- in the move to natural gas that need to be looked at. And again, I am not predicting grid failure or anything crazy like that. I'm talking about pretty much localized issues. But, if you're the power plant on a pipeline that's serving you and it's up for some type of repair under an EPA regulation or a FMSA regulation, or you're being served by a storage field, well, facility, whatever you want to call it in various locations it has a different name, that may merit some additional communication between the electric utility industry and the natural gas provider. Some of that is not in the system the way we think of the electric utility industry today. There were lots of discussion that were fascinating and way over my pay grade yesterday about new tools

and methodologies for communications between electric utilities in terms of cyber and other things. We may need to start to be creative about similar types of communication systems and routinize systems between the gas providers and the electric utility industry. You may not be aware that FMSA has a whole slew of regulations or new requirements of the storage industry for natural gas, and it's not clear to me whether all of the existing, 300 or so existing storage locations across the country will meet all of those standards immediately or whether or not they have to be under some form of repair. I'm not in any way suggesting that there's a big problem. It might be a tiny issue. But wouldn't it be nice if we all knew that?

And lastly, I'd like to offer a recommendation for some suggestions as a follow-up to the hurricanes. I do work and am familiar with one electric utility. I'd rather not say who. But they are dealing with some issues right now as a follow-up to the hurricane and I'd like to give

you this example. This particular utility had some higher sulfur diesel fuel in a tank. This community has not has gasoline available for any trucks or any individual cars in that community since Saturday. This utility reached out to US EPA and asked if they could use the higher sulfur content diesel not in generation but to power the trucks to get the lights back on. EPA said we'll get back to you. To EPA's credit, they were very efficient. They came back and said there was a precedent set on this under Super Storm Sandy. You cannot. So I just would like to point out that there are some other issues that may be learning experiences for us after the hurricanes, both of them in two states -- three states, excuse me, Louisiana -- that may merit some additional disclosure or education in the same way that DHS and FEMA have improved their systems.

I just wanted to mention that the only consequence to using that higher sulfur diesel in those trucks is it was going to tear up the catalysts. The utility was willing to take on

that responsibility. They would have replaced their catalysts. They sure would like to get the power on as fast as possible. That air pollution, human health consequence is pretty negligible for a few days in a town where people need their air conditioning as we have very much heard in the last hours about that elderly center in a different location. Thank you for your time.

CHAIRMAN ADAMS: Thank you very much, Theresa. I appreciate your comments.

Alison Silverstein. Is Alison still here? I know she had another commitments and I think she was not able to stay for the public comments.

I want to be sure, are there any other people that signed up for public comments?

Thank you very much. I think we're ready for our wrap-up. Are there any other comments from any Members? I wanted to ask the Committee for permission to do something. We had a roll off of a lot of our Leadership, somewhat unexpectedly. Amongst them were Sue, who was

mentioned in her contributions to several other reports; and Paul and Carl. I'd like the informal approval of the group to draft a letter of thanks to our Leadership that has rolled off just so they know we appreciated them.

Is there anyone that objects to my taking that action?

Thank you very much. I thought we had a very worthwhile meeting. I'm just amazed at the quality of the presentations of the various panels. I do hope we will think about, all right, we've gotten this information. Now what are we going to do with it? And I'm going to repeat again my recruiting efforts for the Subcommittees. Please, all of you, be signed up for a Subcommittee.

Thank you for coming and participating. If there's no objections, I'm prepared to adjourn.

We are adjourned. Thank you.

(Whereupon, at 12:50 p.m., the PROCEEDINGS were adjourned.)

* * * * *

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, 2020

Notary Public Number 351998