BEFORE THE

FEDRAL ENERGY REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - - x

In the Matter of: :

RELIABILITY TECHNICAL : AD17-8-000

CONFERENCE :

- - - - - - - - - - - - - - - - - - x

Room 2C

Federal Energy

Regulatory Commission

888 First Street, NE

Washington, D.C. 20426

Thursday, June 22, 2017

The technical conference in the above-entitled matter was convened at 9:30 a.m., pursuant to Commission notice, when were present:

FERC COMMISSIONERS:

ACTING CHAIRMAN CHERYL A. LA FLEUR

COMMISSIONER COLETTE D. HONORABLE

FERC STAFF:

MICHAEL BARDEE, (Presiding)

ARNIE QUINN

JIGNASA GADANI

ROGER MORIE

LARRY PARKINSON

LEE ANN WATSON

JOSEPH MCCLELLAND

DAVID ORTIZ

MATTHEW VLISSIDES

MARTIN KIRKWOOD

JONATHAN FIRST

JAMIE SIMLER

ANNA COCHRANE

NANO SIERRA

CYNTHIA POINTER

MARK HEGERLE

LODIE WHITE

ROBERT CLARK

PANEL I: OVERVIEW ON THE STATE OF RELIABILITY
GERRY CAULEY, President and Chief Executive Officer, North American Electric Reliability Corporation
PATRICIA HOFFMAN, Principal Deputy Assistant Secretary and Acting Assistant Secretary, Office of Electricity Delivery & Energy Reliability, U.S Department of Energy
CHAIRMAN ASIM HAQUE, of the Public utilities Commission of Ohio representing NARUC
CHARLES KING, Vice President and Chief Information Officer, Kansas City Power & Light Company on behalf of EEI
STEVEN WRIGHT, General Manager, Chelan Public Utility District on behalf of Large Public Power Council
BABAK ENAYATI, Lead R&D Engineer, National Grid on behalf of IEEE
JOHN TWITTY, Executive Director, Transmission Access Policy Study Group
JOHN HUGHES, President and Chief Executive Officer, Electricity Consumers Resource Council
PANEL II: INTERNATIONAL PERSPECTIVES
BRIAN HEWSON, Vice President, Consumer Protection & Industry Performance, Ontario Energy Board
COMMISSIONER MARCELINO MADRIGAL, Mexican Energy Regulatory Commission
KLAUS DIETER BORCHARDT, Director for the EU Internal Energy Market, Directorate-General for Energy, European Commission

PANEL III: THE POTENTIAL FOR LONG-TERM AND LARGE-SCALE DISRUPTIONS TO THE BULK-POWER SYSTEM

MARK LAUBY, Senior Vice President and Chief Reliability Officer, North American Electric Reliability Corporation

DEDE SUBAKTI, Director, Operations Engineering Services, California Independent System Operator

MICHAEL KELLY RIVERA, Los Alamos National Laboratory

DR. GEORGE H. BAKER, Senior Advisor, Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack

RANDY HORTON, Senior Program Manager, Electric Power Research Institute

THOMAS POPIK, Chairman and President, Foundation for Resilient Societies

SYLVAIN CLERMONT, Director, Reliability Standards and Regulatory Compliance, Hydro-Quebec TransEnergie

PANEL IV: GRID SECURITY

MARCUS SACHS, Senior Vice President and Chief Security Officer, North American Electric Reliability Corporation

MANIMARAN GOVINDARASU, Professor of Computer Engineering, Iowa State University

MICHAEL ASSANTE, Director Critical Infrastructure and Curriculum Lead for ICS/SCADA, SANS Institute

GREG FORD, President and Chief Executive Officer, Georgia system Operations Corporation

DAVID BALL, Director, AEP Transmission Dispatching, American Electric Power

NATHAN MITCHELL, Senior Director, Electric Reliability Standards & Security, American Public Power Association

COMMISSIONER ROBERT (Bob) SCOTT, New Hampshire Public Utilities Commission

BRANDON WALES, Director, Office of Cyber and Infrastructure Analysis, U.S. Department of Homeland Security

P R O C E E D I N G S

(9:30 a.m.)

MR. BARDEE: Good morning everyone. I'd like to thank everyone who's here today and listening outside of the building, and especially thank our panelists, both on this panel and later in the day, for being here and submitting the testimony they've already sent us and for the remarks they'll make today and being available to answer our questions.

Just as a little bit of background, about a little more than 10 years ago Congress approved Section 215 of the Federal Power Act and gave the Commission the authority to approve and enforce mandatory standards for reliability of the Bulk Power System. And since then, we have worked with NERC in this process of adopting and then enforcing the standards.

NERC, through it's regional entities, has really taken the ore on all of that and it's been a good working relationship and I think at this point it's fair to say we have good set of standards. With that, though, there remains work to do. During today's conference, we're going to touch on three areas to explore how we're doing on the reliability of the Bulk Power System and whether there are areas where we need to pay more attention or do more work.

The first panel is going to start with an

overall assessment of the state of reliability, the major issues that we're facing right now. The second and third are going to address emerging issues, both internationally and then in the United States, and the last panel will be on cybersecurity of the grid.

Let me go over just a few housekeeping matters. First, there's no food or drink allowed in the Commission meeting room here, except for bottled water. We would also ask you to turn off your cell phones. We do have a way for people to use Wi-Fi here. There's a piece of paper out on the table outside with the instructions for how to use Wi-Fi, just like that. It says "Guest Wireless Network Rules of Behavior." So if you want to get that a little later and follow that, you'll be able to use the Wi-Fi here.

I would add, though, that if you're using your devices on Wi-Fi, you're not paying attention to us.

(Laughter)

MR. BARDEE: So recognizing that we are a little time constrained, we are going to ask the panelists to limit their oral remarks, generally, to four minutes. There's a clock down here to help you with that. There are a few exceptions because Mr. Cauley is going to be doing the presentation on the overall state of reliability based on NERC's report. We've allowed him a little more time, as we will for our international speakers on the next panel.

Let me just read a statement that is now part of our opening at all the Commission meetings here in the Commission Meeting Room. Members of the public are invited to observe, which includes attending, listening and taking notes, but does not include participating in the conference or addressing the Commission. We will not have a general Q&A with the audience during the conference; however, members of the audience and others may submit written comments in Docket Number AD-17-8.

Actions that purposely interfere or attempt to interfere with the commencement or conducting of the conference or inhibit the audience's ability to observe or listen to the discussions, including attempts by audience members to address the Commission while the meeting is in progress are not permitted. Any person engaging in such behavior will be asked to leave the building. Anyone who refuses to leave voluntarily will be escorted from the building.

So with that, let me turn, first, to Acting Chairman LaFleur for any remarks she may have.

CHAIRMAN LA FLEUR: Thank you very much, Mike, and good morning everyone, very happy to have you here. We have a great lineup of panelists and I've read great pre-filed testimony and happy to have everyone in the audience. It's not only exciting to have people in the

Commission Meeting Room, but is even under normal circumstances, I think, one of my favorite days of the year because it's such a great discussion.

I enjoyed reading the pre-filed testimony and the state of the reliability report. Thank you, Gerry. I just wanted to outline three macro topics, three things that I hope to get from the day as we think about these topics and think about where we're going reliability for FERC 2.0 that will be joining us soon and we'll be moving to the other side of the table again.

First, is where we are in the standards process? As Mike said, we're 11 years into Section 215 and the ERO Enterprise, so where are we? Have we reached steady state? Are we in steady state? Are there emerging issues that we need to focus on and really build up the standards? These are not mutually exclusive, but it might be complementary, or are there ways in which we need to streamline or reduce the standards.

I saw some testimony from some people about selective enforcement based on whether the standards posed a risk to bulk system reliability. Well, all of the standards are supposed to be need for reliability. So if there are standards are not needed for reliability, where are we on the standards? I'd like to get a sense of where we are and where we should be going in a macro sense in the body of

standards.

Secondly, I want to think a little bit about priorities going forward. I always say given the rather unique structure that Congress gave us between NERC and FERC, the success of our reliability effort really depends on our having shared priorities. So as we address emerging issues, be they related to grid security or transformation of the resources on the grid, what should NERC and FERC 2.0 be working on in the coming year between now and when we have our next conference?

And as we look at those issues, what tools should we be using because standards is a tool, but we have assessment and the data work and all of the analysis that NERC and the Commission can do. Voluntary collaboration is another tool and how can we balance sticks like the standards or mandatory rules -- you know mandatory things we put in interconnection agreements, with carrots like market structures to get what we need on the grid. You know which of our tools should we be using to get from here to where we need to be in the future.

And thirdly, I want to focus on resilience, and I know the afternoon panel is really bore in on that. Resilience seems to be the word of the day. Sometimes I think it means different things to different people. To me, resilience means the ability to recover if something bad

happens.

That true, you try to have resilient kids when you're raising children. I like to brag that FERC is resilient because we've been through a lot in the last several months, in the last couple years, and so an institution can be resilient and the grid can be resilient if it can recover if something bad happens. So we talk a lot about the solution against all hazards is building up the resilience, and I don't like to say "resiliency." I know some people put a "Y," but we don't have time for that.

The resilience of the Bulk Electric System does it come from design? Should we be designing it in a different way to build in more redundancy or optionality or ability to island? Does it come from our spearing strategy, things like grid assurance and building on that? How about standardization? There's a law that I have to mention that at every Reliability Tech Conference. If we had more standardization of design and equipment it would be more resilient. And those are some of the things I want to talk about this afternoon. How we really build up resilience, whether we're talking about GMD, EMP, cyber, or anything else. And of course, in all of these cases how can FERC support it.

There's going to be a lot of competition for airtime at FERC, but reliability is job one and this will be

one of the first things we're talking to our new colleagues about and hopefully we'll have some ideas coming out of today about what the priorities should be. Thank you very much.

MR. BARDEE: Thank you Acting Chair LaFleur. Commission Honorable.

COMMISSIONER HONORABLE: Thank you, Mike. Good morning everyone. I was mentioning to a couple of gentlemen before we started that this is our annual reliability party and I'm glad that you all attended.

I noticed we don't have as many people as we had at our markets tech conference, but that's okay. What we have here today are the people who are very serious about this work, who are committed to, and we're going to roll up our sleeves and be as technical as you would like. So this is the place for energy nerds and geeks, I would suggest.

I'm really glad that we're all here gathered this morning to focus on what I call the bread and butter of what we do here at the Commission and that is ensuring the reliability of the Bulk Power System. And I especially want to thank Mike Bardee and staff especially for your leadership and hard work in pulling together this conference and leading until our colleagues join us whenever they will join us and I hope it will be very soon.

I'd like to especially mention Lodie White, who

has worked so hard in pulling all of this information together. I want to thank each and every one of our panelists. A number of you are repeat performers and we're grateful for that. Thank you for the work that you do each and every day and also the prospectus that you bring and the willingness that you have to share it with us. I especially want to thank our international colleagues who are joining us. We look forward to that discussion every year.

As I often say, it's a new day here at the Commission and this isn't our parents or grandparents' grid any more. When we used to think about how the grid operated, I believe that we thought more about the cost to produce it. Do we have enough capacity to transmit it where it needs to go? But while those are still crucial issues in my mind, we also have to worry about a whole host of other issues that we may not have thought about 10 or 15 or 20 years ago.

More than ever utilities need to be concerned now with where and how power is moving and ensuring that we have adequate voltage support, frequency response, inertia. And while we always knew that these aspects were important in moving energy with the dynamic shift in resources and differing attributes of increasingly abundant resources, such as renewables, we must pay careful attention to these characteristics now. We also are having to pay greater

attention to ever-changing cyber and physical security threats as well as electromagnetic pulses and geomagnetic disturbances.

Also, we are more focused on technological advancements and diversity of resources, which have both created new opportunities, but I would suggest they're also equally creating new challenges for us and it really requires us to elevate our game, so to speak, but also the ways in which we work together. And that's why today's discussion is so important in my mind, given the profound changes occurring in our electric system, this is an opportune time to take stock of the progress we've made, where we can improve, with a view of what lies ahead.

The NERC's 2017 State of Reliability Report -- thank you, Gerry and colleagues -- raises a number of issues for us to consider and I look forward to hearing from our panelists about what's working well and more importantly, what we can do better. This isn't a time, in my mind, for us to come together and pat ourselves on the back. It's a time for us to take stock of where we are and more importantly, where we need to be and how we get there together.

I want to take a moment, if I might, to thank Gerry, Janet, Marcus, Mark, and all of our colleagues at NERC for the dedication that you bring each and every day

and all the regional entities who carry out this important work so well. I've greatly appreciated in my tenure here the opportunities to visit with you, Gerry and your team, but also to spend time at NERC MRC and board meetings, which I admit were a little overwhelming my first time; but also at CERC's meeting with reliability first. Sitting in on MISOP's discussions at SPP, and with CERC, and I've been delighted to host a number of you here at FERC, including the MRO, WEK, PEAK, and others.

Thank you most of all for taking time to educate us and letting us know about the current state of play, but I also see the fruit that this labor brings and I see that we've increased our levels of coordination and decreased MISOP's, we'll hear about that today. We have a stronger focus on cybersecurity and physical security and a greater level coordination among stakeholders in the NERC process and in our working relationship with NERC and I'm really grateful for that and I want to thank you all for exhibiting such a strong commitment to this work.

But we know that our work is not done. We must continue to remain vigilant, to be nimble, responsive, and to remember that no matter what the industry looks like in the future our jobs at their core remain the same, to ensure electricity is delivered safely, reliably, and affordably to the consumers that we serve.

I hope that throughout this day, and I thought it was interesting that yesterday was the summer solstice and the longest day of the year. I wish this meeting was yesterday because we never have enough time to cover all the things we want to talk about, but I'm particularly interested in, and I mentioned to Pat Hoffman before we began, three key areas that I think we need to pay attention to going forward.

Number one is cybersecurity. And I know that's a priority for so many of you, but I think -- and I think everyday consumers are more aware of how cyber threats are growing and evolving and it really requires a new level of awareness education and commitment and an ability to defend our facilities and resources.

Number two is gas/electric coordination. I think as we're seeing such a dynamic shift in the energy mix -- and I applaud FERC long before I arrived -- focus on gas/electric coordination. And when I was a Commissioner along side Chair Haque, we engaged diligently with our FERC colleagues on the issue of gas/electric coordination. That issue will only become more challenging for us, I suggest, going forward.

Last, but not least, is an area that I've seen really resonate in the pre-filed comments that we will hear about today during the tech conference, and that is our

state and federal coordination with our regulatory colleagues. I especially want to thank our colleagues at NERC. Thank you, Chairman Haque. My goodness, you're wearing many hats as you elaborately stated in your comments. We need for our state colleagues to be right there at the front lines with our federal colleagues in carrying out this important work. And I look forward to our discussion today. Thank you.

MR. BARDEE: Thank you, Commissioner.

Now we'll turn to our panelists for their opening remarks, starting with Gerry Cauley.

STATEMENT OF MR. GERRY CAULEY

MR. CAULEY: Thank you. And good morning Chairman LaFleur and Commissioner Honorable and I guess virtual Chairman Bardee for today and FERC staff and fellow panelists.

I want to thank the Commission for holding this annual Reliability Technical Conference to discuss reliability results and priorities. I'd like to offer my thoughts on four key points from NERC's fifth annual State of Reliability Report, which was issued this past week.

First, low power system reliability remains very high. It continues to show year over year improvement. Industry has been very responsive to our risk-based approach and has been shifting resources to fix the most critical

changes to reliability. In 2016, we once again saw no category four or five events and only two category three events. Equipment failures continue to have the highest positive correlation to outage severity or impacts. Relay miss operations and human error are second and third. The number of transmission line device failures and human error reports in 2016 both increased, although the impacts of each declined. We believe the increase in reported incidents is due to better cause analysis, which also resulted in the corresponding reduction in reporting of unknown causes.

The reduction in relay miss operations continues to be very encouraging. 2016 saw the miss operation rate decline from 9.5 percent to 8.7 percent. A second point is that I believe NERC standards and risk-based compliance are having a positive impact on reliability. On June 18, on Father's Day, we passed the 10-year anniversary of mandatory standards. These standards have had a major impact on reducing risks in areas such as vegetation management, situation awareness, operator training and system planning and modeling.

Over time, we've seen a dramatic decline in the number and the severity of compliance violations. I believe, however, it may be time to focus again on streamlining the requirements to ensure the investment and compliance is commensurate with the reliability gains. We

also want to continue working to ensure that compliance becomes integrated into reliability operations and is not seen as a separate administrative burden.

A third point is that changing technology and resource mix are reshaping reliability at a pace we've never seen before. We've seen the introduction of digital technology operating in microseconds being integrated with traditional protection and control systems that operate in cycles and seconds.

A clear example occurred last August 8, 2016, during the Blue Cut fire in California. In the past week, NERC published a technical paper and a Level 2 alert describing how 1200 megawatts of solar power quit producing at a critical time because the invertors were interpreting transit voltage and frequency values from line trips as the actual system frequency and voltage. I want to applaud the recent response of the California ISO to require additional reserves in the market to address uncertain response from some inverter-based resources.

NERC has been working with renewable vendors to adjust inverter settings and to provide effective ride through capability and the vendors, I assure you, are being very cooperative with us on this issue. I also feel we may need to clarify our standards to ensure that when new technology gets introduced into the system that the

terminology that we used to think was fine is clear with regard to the new technology.

We're also focused on a number of other emerging reliability risks and I'll leave those primarily to Mark Lauby on the next panel, but they are the impact of distributed energy resources on the Bulk Power System. The dependence on natural gas, particularly, critical storage and pipeline facilities, and the adequate provision of essential reliability services when large rotating machine which used to be base loaded are now not being dispatched.

My fourth point is that cybersecurity has become the most important risk that we face. Today I believe we've seen exceptional performance with no electrical system outages or serious events, but as we will hear in a later panel from Mark Sachs the threats are becoming more serious and at an alarming rate. The 2015 and 2016 attacks in the Ukraine show that the tools for nation-stayed disruption of power grids have been fully developed and tested.

The recent announcement of crash override, a very robust threat to industrial control systems and operating systems, is of very serious concern to me. NERC issued an alert to industry last week with proposed mitigating measures for industry. Wannacry and the Internet Things attack in recent months are also likely to affect us, but more in the corporate side, but those threats remain

serious.

I want to thank you for your time today and I very much look forward to your questions. Thank you.

MR. BARDEE: Thank you, Gerry. Next, we have Patricia Hoffman from the Department of Energy.

STATEMENT OF MS. PATRICIA HOFFMAN

MS. HOFFMAN: So thank you Chairman LaFleur, Commissioner Honorable and the Commission staff. Thank you very much for your leadership. Good morning and it is a pleasure to be here to participate today at the technical conference on the state of electric reliability. I appreciate the opportunity to express the views of the U.S. Department of Energy.

As Gerry has mentioned, the U.S. electricity sector is in the midst of major changes and I see little reason to expect that this process will slow down or that we will reach some new equilibrium any time soon. On the contrary, the process of change that we are experiencing today will probably continue. Accordingly, I think the fundamental challenge is now to understand this process and to manage it with proper investments so that our nation's electric infrastructure remains reliable, affordable, and secure.

Before I highlight some topics of concern for this Commission, I would like to take a moment to reflect on

some accomplishments by industry that are providing value to system reliability. Lessons learned from the 2003 blackout highlighted the need to develop better, real time tools for operators and reliability coordinators, improve system modeling data and data exchange practices, require the use of real time synchronized data recorders, and tighten communications protocols, update communications hardware where appropriate.

Lessons learned from the 2011 Southwest blackout highlighted the issues from planning, modeling, and remedial action schemes. Recent hurricanes have demonstrated the need for improvement in communication, automatic switching, and outage management systems. A significant amount of research development and deployment has advanced most of these recommendations, including the development and deployment of PM used, advanced meters, outage management systems, real time tools for operators, but unfortunately, there are still some recommendations that are still under development, such as dynamic remedial action schemes, improved and faster modeling systems with great fidelity.

The Electric Sector Coordination Council reiterated the need for improved communications and redundancy in communications, but as Gerry has stated, the performance of the system is improving overall; however, one must keep close watch on regional issues developing. So

with respect to this panel today, there are a couple of things I'd like to highlight.

Physical and cybersecurity, utilities and system operators need to continue the efforts to identify data, facilities and systems that are essential to the reliability of the system and take reasonable steps to harden them. Mitigate the reliability risks associated with rising gas and electric interdependence. The Aliso Canyon Event involved the functional loss of a major underground natural gas storage facility in Northwest Los Angeles, which has lead to increased reliability risk to the Los Angeles area.

The third area is the need for planners to build more flexibility in optionality into their systems, both in the short term and the long term. The uncertainties the assistant planners must take into account have multiplied in recent years and this condition is not expected to change any time soon.

With respect to data and data analytics, without sustained data and visualization, long-term grid reliability can be compromised. With respect to diversity of generation and reliability, the electricity grid has undergone a transformation as new technologies, changing economics, and shifting customer behaviors and government policies are driving change and we must identify the services expected from the generation fleet in the United States and the

appropriate compensation. So with respect to distributed energy resources, the trend is going towards more decentralized electric grid with greater variability of resources providing powers in the ways that today are much less predictable, hence, the ERs are challenging to our traditional approaches to planning operations and raise new questions about how to control, coordinate, and optimize a large number of diverse resources.

And the last thing I'd like to mention is the reliability study. Earlier this spring, Secretary Perry asked DOE staff to initiate an internal study to explore the issues central to protecting long-term reliability of the electric grid. Secretary Perry asked the staff to explore three issues: the evolution of wholesale electricity markets, including the extent to which federal policy and the change in electricity fuel mix challenge grid reliability, whether wholesale capacity markets are adequately compensating attributes such as one-site fuel supply and other factors strengthening grid resilience and the extent in which regulation and legislation affect early retirement of base-load generation plants.

While recommendations are expected from the final report, it is likely that several areas related to reliability will be identified for further research and study. So with that, I'd like to conclude my comments and

thank you and look forward to questions.

MR. BARDEE: Thank you, Pat. Next, we have Chairman Asim Haque from Ohio.

STATEMENT OF MR. ASIM HAQUE

MR. HAQUE: Good morning. Chairman LaFleur, Commissioner Honorable, and staff, thank you for inviting me to participate in today's technical conference. My name is Asim Haque and I am the Chairman of the Public Utilities Commission of Ohio. I have the privilege of serving on the Board of Directors of NARUC and I'm also one of two state government sector representatives elected to the Member Representative Committee of the NERC, actually an opportunity that was provided to me by then-President Honorable. So thank you -- I think thank you.

It is in this total capacity, Chairman of the State Commission, representative of NARUC and of the NERC MRC that I present these remarks today. These remarks are meant to simply inform the Commission on topics related to NERC's reliability endeavors that are foremost on the minds of the states. These topics include distributed energy resources and their collective impact on the Bulk Power System, reliability impacts associated with the retirement of base-load resources and efforts to incorporate costs into the NERC's standards process.

Before I elaborate on these topics, I would like

to first recognize the diligent work of NERC. NERC has the difficult and highly technical task of ensuring the reliability of the Bulk Power System and it performs very admirably in that task. State commissions also appreciate the strong relationship we have developed with NERC.

The rapid advancement of technological innovation on the electric grid is causing many states to launch grid modernization endeavors. Ohio, in fact, recently launched a comprehensive grid modernization endeavor entitled "Power Forward." Power Forward is built upon to pillars, innovation, both technologic and regulatory, and the concept that this innovation must serve to enhance the customer electricity experience.

As the PCO has learned in Power Forward, innovation associated with distributed energy resources is quickly growing and we expect for this marketplace to continue to expand. Regardless of the path the states take for integrating and compensating these resources, the states understand that they are traversing through somewhat uncharted waters. This sense of the unknown also applies to the intersection of distributed energy resources and the Grand Pack Dunball Power System reliability.

NERC understand this and has proactively created the Distributed Energy Resources Taskforce. NARUC is pleased to be actively participating in dialogue with

members of that Taskforce. They believe that the recommendations in that Taskforce's final report associated with things like data sharing, modeling, and industry collaboration are very, very sensible.

The states understand that the increased proliferation of the distributed energy resources cannot compromise bulk power system reliability. The states and NERC are learning together and the states stand ready to assist. This could take the form of information sharing so that appropriate modeling can be conducted for the recommendation of that Taskforce report. This could also take the form of an effort that produces some type of uniform guidance socialized through NARUC.

There continues to be much dialogue surrounding the changing resource mix and the retirement of coal and nuclear generating plants. Some states are taking measures to subsidize these base-load plants through various state initiatives. These state initiatives have prompted very robust policy debates. Missing from this discussion, however, has been a true scientific analysis to explain reliability risks to the Bulk Power System as these base-load units face potential retirement.

NERC is uniquely situated to conduct this analysis, as the electrical liability organization for North America NERC is capable of examining this issue through

actual science and engineering. NERC conducts special assessments on emerging issues and trends that will influence both power system planning, development, and system analysis and this is one of those items that NERC is considering studying.

Grid reliability should be viewed as a scientific problem and NERC's concept of a special assessment for accelerated base-load retirements could provide concrete data that may serve to inform public policy determinations, thus, NARUC would support and encourage NERC's efforts to engage in collaborative discussions based on the scientific outcomes of that study.

I previously testified that cost should be considered in NERC standard development and implementation and that this would help to foster a culture of reliability excellence. The cost of facility compliance with NERC reliability standards will always be a concern. For state commissions, I am pleased to report that NERC, based on input from its stakeholders, including NARUC, has developed a plan to promote cost analyses in its standards process. NARUC has requested that NERC provide meaning reporting related to the outcomes of these endeavors at least biannually. After NERC's latest proposals are initiated, we would like to know how these actions are tangibly impacting the -- process, if at all. But again, NERC has done a

marvelous job in addressing this.

Commissioners and fellow panelists, thank you again for the opportunity to participate this morning. I look forward to questions.

MR. BARDEE: Thank you, Asim. Next, is Charles King, testifying on behalf of EEI.

STATEMENT OF MR. CHARLES KING

MR. KING: Thank you and good morning. Acting Chair LaFleur, Commissioner Honorable, staff, for the opportunity to be here this morning. Just a brief perspective that I think is important when we have these conversations, electricity's value is measured by its reliability. The significance of reliability has not changed significantly since the times of Thomas Edison first opening the Pearl Street Electric Station in New York City up through the technological advances that have lead us to the modern electrical grid today marked by things such as renewables, distributed generation, smart grid tools that include energy response and then also ideas that were once aspirations of how we would use electricity that are today reality, such as electric vehicles.

However, those innovative transformations, as we all know, that are a part of the electrical grid today have also brought forth challenges to reliability as we've already discussed this morning, and that includes providing

essential reliability services and also, of course, cybersecurity as two of the largest.

I'd like to underscore that when we discuss reliability it's essential that we keep in mind the industry incentive fostered by the very nature of our business. It's simply in our DNA to provide reliable sources of power and deliver that power reliably to our customers each and every day. With or without mandated standards, the industry is focused on providing reliable power. Now the reliability standards are in place to provide a strong regulatory framework that promotes and works to support reliability.

The Commission, NERC, and the industry, I think, have done an excellent job at building and implementing that framework as evidenced by the current high levels of reliability. The reliability risks take on many forms, shapes, and sizes. For example, cybersecurity every day it evolves. It exploits known vulnerabilities, unknown vulnerabilities and we also have innovations, such as those I mentioned a moment ago that give us distributed energy sources.

But as good as the regulatory and standards framework is at promoting reliability and addressing challenges and threats to reliability, the speed at which these risks and threats are evolving creates concerns. Cybersecurity, for example, the threats evolve literally

every day and the process and time it takes to develop a standard and implement a standard may not yield the desired results to mitigate vulnerabilities in a timely fashion.

Today's grid technology continues to rapidly evolve, such as smart inverters. Sometimes those underlying reliability risks cannot be identified and mitigated as quickly as desired, which makes drafting reliability standards and requirements difficult without the time for effective study and cooperative research. While the standards development process is solid and effective, its design does not easily accommodate these emerging, evolving risks that we face today.

In light of this limitation, we need to seek out ways to supplement our current processors and other alternatives. Many in government and the industry, however, have already stepped up to this challenge, for example, the work done by the Electricity Subsector Coordinating Council recently in the area of grid security. The definition and roll out of the cyber mutual assistance model I think is an excellent example of that partnership. That partnership, by the way, between industry and government does not replace the current regulatory and standards development process. It simply offers an alternate path to expedite response and further strengthen the grid.

We encourage the Commission to look for

alternatives to prescribing new or burdensome regulations to addressing these emerging reliability risks. Grid technologies and the reliability risks associated with them are going to continue to rapidly evolve, too rapidly to address them through prescriptive requirements.

The Commission, NERC, and us as industry, we all have a shared commitment to reliably operate the Bulk Power System. That's evidenced by ongoing work to address reliability, improve reliability through regulation, government/industry partnerships, applying lessons learned from events in North America and around the world, and also just the rigor with which we approach addressing new challenges caused by new technology and emerging threats.

So in recognizing industry's responsibility to our shared commitment to sustain and advance reliability, we'll continue to partner with the Commission, bring forward possible solutions, alternatives, different approaches and we look forward to collaborating with the Commission, NERC, and our other stakeholders to discuss these possible solutions as we all work together to protect and advance the reliability of the grid. Thank you.

MR. BARDEE: Thank you, Mr. King. Next, we have Steven Wright, speaking on behalf of the Large Public Power Council.

STATEMENT OF MR. STEVEN WRIGHT

MR. WRIGHT: Thank you for the invitation to appear again today at this conference. We reviewed today a unique law that assumes effective collaboration and communication between industry and government. Through focusing annually on the most strategic issues, this conference is an important element of making the law successful.

I want to start from the perspective that (mic malfunction) -- , managing a number of systems that I've had responsibility for adopting those standards.

To get to the first two points that Acting Chairman LaFleur laid out, we have four primary suggestions for strategic focus for the next year. First, create more compliance management rewards for entities that embrace a risk-based approach to reliability standards. The standards are appropriately a systematic, methodical means for managing a very complex system

In the case of our utility, and I believe most around the country, our compliance management staff and costs continue to grow. Our challenge since the time this conference was originally initiated is how can we get the biggest bang for our buck. The NERC risk-base compliance and monitoring enforcement program encourages utilities to perform inherent risk assessment to better understand impacts the entity has on the Bulk Electric System. And

the CMAP also encourages an assessment of internal controls that an entity has in place to manage reliability risks.

At Chelan and for many of my LPPC colleagues, we chose to go all in on IRA and ICE. There is no doubt in my mind that the resulting knowledge and process management has improved our impact on the reliability of the system. And in fact, our auditors identified us as a top tier performer. What I had expected, though, was that as we better understood and documented our contribution to reliability there would be reductions in compliance management costs.

Now in fact, our audit scope was reduced by 87 percent, making data process go smoother. To this point, though, there has been little reduction in our documentation requirements, which is where the bulk of reliability management costs occur, of the 1,236 requirements and sub-requirements applicable to Chelan four have been identified as eligible for self-logging.

NERC has proposed process modifications that could lead to more rewards for utilities that choose the path of seeking excellence and we encourage FERC to respond positively to these initiatives. We also would suggest that the regions be given more authority to say don't worry about where individual entities' standard implementation is not material to Bulk Electric System reliability.

Second, the use of cost-effectiveness criteria,

NERC is to be commended for their efforts to advance this concept. A lot of good work has been done. But as a knowledgeable friend of mine recently summarized, it's difficult and we still have a long ways to go. We would encourage further dialogue between industry and NERC and FERC to advance these concepts.

An important issue to arise this past year has been supply chain procurement. LPPC believes this problem is real and must be addressed and it's good news that the industry has recently approved a new standard. I'm concerned; however, that fundamental management principles and accountability are at risk of being violated by managing this challenge only through the statutory framework of mandatory standards that apply solely to the electric utility industry. An entity can only reasonably be held accountable for actions that they can control and I would strongly encourage that FERC, NERC, and the industry jointly approach other federal agencies that have cybersecurity responsibilities to develop an overarching strategy that extends beyond the electric sector.

Fourth, any discussion of reliability would not be complete without considering the changing nature of the physical operation of the Bulk Electric System, particularly, in the West were there's a proliferation of variable energy resources. The challenge of managing a

system with increasing amounts of non-dispatchable resources has been understood since at least 2013, but the pace of BERs being added to the system is accelerating beyond previous projections. Actions are being taken and near-term reliability, I believe, is likely not at risk, but as the fleet and grid transform metrics such as a resource adequacy need to evolve.

At this point, solutions beyond the next three to four years addressing in particular the afternoon ramp challenge are not agreed upon or being executed. And we also have to consider alternative means of compensating for needed flexible capacity.

So in conclusion, we should be proud that reliability is getting better, but as with any system there are opportunities for continuous improvement. We commend the Commission for holding this conference on an annual basis and look forward to continuing to work with you.

MR. BARDEE: Thank you, Steve. Next, we have Dr. Babak Enayati from IEEE.

STATEMENT OF DR. BABAK ENAYATI

DR. ENAYATI: Thank you. Good morning Chairman LaFleur, Commissioner Honorable, FERC staff, and my fellow panelists. I thank you for the opportunity to speak at this conference today. IEEE is the world's largest technical

professional organization dedicated to advancing technology and IEEE and its members inspire global community to innovate for a better tomorrow for its more than 420,000 members in over 160 countries in its high cited publications conference psychology standards and professional and educational activities.

As the most active IEEE society in publishing standards, IEEE Power and Energy Society provides the world's larges forum for sharing the latest in technological developments in the electrical power industry and so various policies, regulations, and legislation seek to deliver the environmental objectives for the power generation sector. The North American Electric Power System is becoming more reliant on wind, solar, natural gas, and demand response.

In addition to changing energy landscape in the wholesale market, most of the states in the U.S. have ambitious goals to deploy DER in the retail market as well. Given that DER penetration, including green -- generation is increasing rapidly in the U.S. The impact on the Bulk Power System reliability is becoming more apparent.

In order to avoid reliability violations, supply disruptions, or extensive transmission upgrades, DER interconnection standards need to be updated to allow DERs to support the Bulk Power System during frequency and bulk disturbance, also known as ride through capability. As

deployment of DERs on the distribution system increases, the impacts on the Bulk Power System reliability need to be addressed promptly by updating the standards that govern the technical aspects of the DER interconnections.

Many utility distribution companies in the U.S. have adopted IEEE 1547 standards, which provide a set of technical requirements that each DER shall meet to interconnect to the distribution electric power system. Given that the implementation of IEEE 1547 standard is essential to the Bulk Power System reliability, there are some major challenges associated with the implementation of the standard.

The top two concerns are, number one, modeling. Currently, the tools that are widely used by distribution for utilities for DER interconnection protection studies are not capable of accurately modeling the DERs with the grid support functionalities, also known as advanced DERs.

Number two, concerns related to adverse impact of advanced DER functions on the distribution system anti-island protection and short circuit fault detection. Some distribution utilities are concerned that the advanced DER functions may have adverse impact on the distribution system protection related to the prolong fault and island distraction due to the ride through requirements.

What needs to be done? As the IEEE 1547

standard is in the revision process, IEEE recommends that the Commission collaborates closely with the distribution utilities, the original ISOs to resolve the concerns associated with implementing the DER ride-through requirements. This collaboration will avoid the delay to implement the IEEE 1547 standard once it's officially published. IEEE believes that the Commission and NERC can play a key role in directing those discussions through the regional ISOs.

IEEE Power and Energy Society has the resources and the technical knowledge to help the Commission, NERC, and the regional ISOs to implement the industry standards related to Bulk Power System reliability. And I also want to give you the good news that the 1547 standard passed the ballot last Sunday. So it was open for ballot for a month and it passed the ballot. They are forming a comment resolution team and will address the comments that we received. It was in total about 1,457 comments, so yes, we'll work on those comments and we're targeting the end of this year, hopefully, to publish the standards.

So this concludes my presentation. I will be happy to address any questions you may have.

MR. BARDEE: Thank you, Doctor. Next, we have John Twitty from the TAPS Group.

STATEMENT OF MR. JOHN TWITTY

MR. TWITTY: Madame Chair and Commissioner Honorable, nice to be here today. Mr. Bardee, thank you very much for the opportunity. I am here today to speak on behalf of TAPS. TAPS is an organization that represents transmission-dependent utilities in 35 states. The members of TAPS are joint action agencies and utility operators with direct responsibility for keeping the lights on for their customers.

Because we are transmission-dependent, we are highly reliant on the reliability of transmission facilities owned by others and at the same time many TAPS members are subject to compliance with NERC standards. So we are both supportive of cost-effective actions to ensure bulk system reliability and acutely aware of the increasing cost of new reliability regulations.

I've been in the business now in my 35th year and have experienced two municipal utilities and now at TAPS. I also have the privilege this year of serving as the Chair of the NERC Member Representatives Committee and I was a member of the NERC Reliability Issues Steering Committee. So collectively, this experience has provided me lots of thoughts about customers and reliability.

Let me began by acknowledging the success that FERC and the ERO have had over the past decade and a little bit more. We've collectively kept cascading outages to a

minimum through a period of rapid change in the industry and with technology and I suspect everybody agrees those changes aren't going away. I believe it is important to emphasis that we must be careful to measure reliability against what the Congress wrote.

Outages occur for a variety of reasons, of course, but Congress directed that FERC and its ERO guard against BPS instability, uncontrolled separations, and cascading outages. This focus is particularly important to remember, especially as distributed energy resources begin to play a greater role in today's grid. We must be sensitive to avoid allowing the federal jurisdictions of FERC and NERC to creep into local distribution systems of the operating utilities across America. It should not be the intent of FERC to undercut state and local regulatory mechanisms that are best designed to serve the need of local communities.

I would also like to discuss the cost associated with the requirements of standards that have implemented since they became mandatory with passage of the Energy Policy Act of '05. When I served as general manager of City Utilities, I used to say to our industrial customers that we could guarantee 100 percent reliability, but they wouldn't want to pay that much. The engineers in the room always used to say you really can't do that and we might all agree

about that, but the point is the higher degree of reliability delivered the higher the cost.

We all understand the importance of competitively prices energy and its impact on the competitiveness of our customers. After all, it is the commercial and industrial customers we serve who provide jobs in our community. I also think we need a renewed paragraph 81 effort. When FERC first suggested that requirements and standards be reviewed to make sure we weren't duplicating effort or undertaking efforts with little benefit, it was a welcomed sign.

Earlier this year, Gerry Cauley mentioned that very thing and we support it in the strongest possible terms. Once that first effort was underway, we were hoping there could be a significant number of requirements that could be retired. And while there are successes to be celebrated, we believe there are even more requirements and standards that should be carefully reviewed to see how much value they bring.

Let me close by stating the obvious, cybersecurity and cyber issues, generally, have given us perhaps a greater threat than any we face. Many positive steps have been taken to help address these issues with the EISAC and ESCC working actively to help prevent widespread outages. Again, TAPS is most supportive of these efforts,

but we must be careful about the costs associated with this work and carefully examine whether tools available to FERC and NERC other than reliability standards are better suited to promptly addressing evolving cybersecurity threats taking full advantage of quickly changing technology and lessons learned.

Again, thanks so much for the opportunity to be here today. Look forward to the conversation.

MR. BARDEE: Thank you, John. And finally, we have John Hughes from ELCON.

STATEMENT OF MR. JOHN HUGHES

MR. HUGHES: Thank you Michael and Commissioners. It's a privilege to be back here. And on behalf of my members, I want to state that a few things are as important to ELCON members as reliable electric service. They can't do business without impeccably reliable service.

I also want to start on a positive note by thanking the leadership of the ERO Enterprise for the access that they've given to large manufacturers and particularly NERC staff, the very capable Board of Trustees and the regional entities. I think I can state that NERC is no longer a utility club.

I especially want to compliment NERC and the regional entities for adopting results-based standards development and the risk-based approach to compliance

monitoring and enforcement. This has significantly reduced a regulatory burden of NERC standards on our members that are registered entities and is also, I believe, prevented frivolous registration by members that provide no risk to the reliable system.

ELCON members have a unique perspective on reliability issues. Our definition of reliability is much broader than what was in Section 215 and by that I mean that we are subject to the dual jurisdiction of states as well as the federal laws and many manufacturing facilities are interconnected that both the BEF system as well as the distribution system and events on either one of those systems can impact the manufacturing process.

We have an overriding concern about the current changes in the industry with the adoption of more intermittent resources and DER distributed energy resources, but we are grateful for the fact that at least at the BES level NERC is addressing these concerns and we hope that the Commission will support these efforts by NERC.

With the remainder of my time, I want to focus on two specific areas of concern. First, in the interest of the canary in the mine shaft, several of my members are reporting an increase in power outages that do material damage to their manufacturing facilities. And I don't have enough degrees of freedom of data on this to really

definitively identify a trend. They seem to be scattered throughout the United States and the best I can tell they're kind of 50/50 at both the BES level and the sub-BES level.

While I'm continuing to work with my members to try to identify more specifically what's going on, obviously, these are not associated with any type of wide, cascading outage. These are all local events. I keep hearing from quite a few of my members that they're experiencing greater voltage problems outside the fence of their manufacturing facilities. Of particular concern is they're getting no feedback from their local utility on what's causing these problems.

A second concern deals with a trend that there's an expectation that manufacturers should have their manufacturing process dispatched for the purpose of providing BES reliability and they can't do that. There's a term called "demand flexibility" that's used by advocates of a carbon-free society to explain why they think that it's really the customers that should be providing the reliability to the system rather than utilities.

We disagree with that mindset. Most manufacturing facilities, especially large ones, are inflexible. And I would note that NERC has -- excuse me, FERC has a NOPAR pending on primary frequency response which

goes down that path and we would like to see a speedy resolution of that issue.

And again, thank you for the opportunity to appear and I look forward to your questions.

MR. BARDEE: Thank you, John. Thanks to all of our panelists. Let me turn first to Acting Chairman LaFleur for questions she may have.

CHAIRMAN LA FLEUR: Well, thank you Mike and thank you to all the panelists. I love this seat. I'd rather sit where Mike is sitting, but we have a great view here.

Okay, so many ways I could go. I think I'm going to start with the question I posed in my opening comments and was also raised by Steve Wright's comments. And I want to call out Steve Wright as my memory being the person who suggested having these conferences in 2010. So in some of your comments at that time, if I recall, about more interaction with Commissioners and so forth, so thank you.

Steve, John, John Hughes -- John Twitty and John Hughes all talked about I'll call it risk-based selective enforcement of standards and being more risk-based in the way we conduct compliance with compliance -- whatever CMEP stands for, Compliance Monitoring Enforcement Program. And I tried to be supportive of NERC's desire to be more

risk-based in enforcement, but I had this competing feeling of like why do we have standards that we don't want to enforce?

If there are standards that don't relate to -- that are, in Steve's words -- we should remove from the list of standards if you've had this inherent risk assessment standards that are needed for grid reliability. If you have standards that are not needed for grid reliability, why are they standards?

Are there things -- are there documentation of other standards you would propose streamlining because it comes out as like after the fact to kind of only selectively enforce, but then you always a fear you might be enforcing the wrong ones or the mechanisms you use to figure out what to enforce with whom are not sufficiently sensitive. So is there a problem with the complexity of the standards? Is there something we should do 11 years in to adjust this rather than backing off on enforcement?

And I'll maybe start with Steve, but by Gerry or anyone to comment.

MR. WRIGHT: I think there are two ways to come at this. You know one is very consistent with what Gerry's talking about and one is a bit new.

So a few years ago, I can't remember exactly how many, NERC were through the paragraph 81 process to review

all the standards and a couple of the panelists here and Gerry, I think, said there may be time to revisit that and see where we can get and that was as useful exercise. I described it as modest, but significant changes that were made to the standards at that time to review and understand just what's working and what's not providing as much value and it could well be time to review that. It depends on which standards you're talking about. I don't that we're really quite ready on cyber standards yet. We're probably a year or two away.

CHAIRMAN LA FLEUR: I would agree.

MR. WRIGHT: So you have to look at where the standards are in terms of their maturation process and then decide whether it's time to go through that paragraph 81 process.

The part that I'm suggesting that's a bit different is we put in place IRA and ICE in order to be able to understand the impact of each registered entity's impact on the Bulk Electric System. And that has really been good work. I have to tell you it was hard. It was very difficult, but I think it was extremely valuable to do that. But now what we have is the opportunity to look at each registered entity and standards are one size fits all. And now with IRA and ICE, we have the ability to look at the impact each registered entity has on the Bulk Electric

System and determine whether the one-size-fits-all standard is necessary in terms of its full application to that entity or not.

In order to do that, it would require more authority to be given to the regions because there's no way, I believe, that NERC could be able to manage that process for all of the registered entities, but just take a look and say, okay, do we need the full application of this standard for this entity, given some entities are at that big impact and others have a much smaller impact.

CHAIRMAN LA FLEUR: Well, I fully supported the paragraph 81 effort, which I think Commissioner Norris first suggested, but I thought of that as much more kind of looking through and making sure we didn't accidentally have duplicates or there were little things we could shave at the edges.

I just want to understand. Drawn to its logical conclusion, Babak, who is sitting next to you, from National Grid, would have a different set of standards or Southern would have the highest standards because they're bigger and someone little would have fewer standards. Is that kind of what you're saying?

MR. WRIGHT: I don't think it's necessarily bigger or smaller. This is the great thing about inherent risk assessment. It allows you to look what the impact of

the particular facilities that you have what's their impact on the Bulk Electric System, so it could be that you might be a small entity, but you could have a big impact on the Bulk Electric System.

CHAIRMAN LA FLEUR: So if you don't have a big impact, then we loosen up on something we might require someone else to do, in concept.

MR. WRIGHT: And it wouldn't be tied to the entity itself. You'd have to go through standard by standard, right? So it could be that the individual piece -- you know go back to the Southwest outage. Clearly, there were facilities on the IED system which were really important to the Bulk Electric System.

CHAIRMAN LA FLEUR: I thought of them when you said that.

MR. WRIGHT: I think we probably all do candidly, is thinking through that, so you wouldn't be able to say, okay, you're a small guy; therefore, you have no impact. You'd have to go through and say what is that facility that you have? How does that relate to the standard? How important is that to the Bulk-Electric System?

CHAIRMAN LA FLEUR: So you're talking quite a bit of customization of the standards.

MR. WRIGHT: Yes. And that's why I said would

require authority to be given to the regional entities in order to be able to go through that. I don't think that could be managed ^^^^

CHAIRMAN LA FLEUR: So think paragraph 81 is enough to do any kind of macro streamlining we need to; that that's enough of a tool.

MR. WRIGHT: So our experience with paragraph 81 was a favorable one. I think it worked well. And again, that's probably something that should be repeated every so often to just to go back through and say how has the system evolved and what have we learned.

CHAIRMAN LA FLEUR: John?

MR. TWITTY: Well, Madame Chair, I think it's important to continue that paragraph 81 effort. You know when it first started there was lots of enthusiasm with that and I would certainly agree with what Steve has said here.

The intent then, as I understand it, Gerry certainly can correct, is that we would move that process to where were writing new standard. We're writing them with the thought that we're going to review what's in the field of vision and in that process we're going to make sure that going forward we're not duplicating, that we have cost-effective standards.

I really would be supportive and I think TAPS would be supportive of sort of a renewed effort to start all

over again. I think Steve's comments about internal controls and inherent risks is particularly important for TAPS because we're small members, by and large. And I say often our members might do something that might turn the lights out all across town, but it's not going to feed into the Bulk System. You may catch heck at the grocery store or church next Sunday.

CHAIRMAN LA FLEUR: Or when you see John Hughes.

MR. TWITTY: Yeah. Hey, John, the lights are out at Alcoa today, happy to know that, really to tell you why. So I would really like to see a brand new effort and to further recognize that not one size fits all.

CHAIRMAN LA FLEUR: John Number Two.

MR. HUGHES: Briefly, one of the nice thing the NERC does -- actually, it's something that its Board does is seeks policy input from the MRC and on a quarterly basis in advance to the Board members. And one of the recommendations that we put forward recently I think touches on what you're getting at, and that is we need some sort metrics on the requirements of each standard that tie the requirement to the quality of the reliability or improvements in the reliability. And I think it's safe to say that no standard is written perfectly and if we had more time and more people to work on them we would want to improve them. But maybe a metrics of this type might be a

way of identifying which ones could be rewritten for more effectiveness and really identify and truly reduce the risks.

CHAIRMAN LA FLEUR: Gerry.

MR. CAULEY: Thank you. I appreciate the comments that fellow panelists in wanting to streamline and get more efficient around compliance and standards.

One of the pivots that we're in the process of making is probably not widely known, but we're preaching around the ERO Enterprise is risk-based compliance standards is moving to sort of how do you prioritize the most important reliability issues to a new concept, which is basically fearless focus on any effort you can do to prevent the next outage and use the standards for that and use a compliance activity.

So if an activity is not contributing to preventing the next failure, then it's not as helpful. You know so there's some value in standards and compliance for punishment if somebody does really bad behavior. We're making that pivot across NERC and the Enterprise.

So that points out a few things. First of all, I do believe that there's an opportunity now to do a concerted review of the standards to make sure they're all contributing to preventing the next outage.

CHAIRMAN LA FLEUR: By definition, they should

all have something to do with preventing cascading outages on control separation.

MR. CAULEY: Exactly. And given the asymptotic approach, we've seen some good reliability and the crunch on revenue and resources I think it's time to go back and look at it again, not in an incremental five-year process, but maybe one more time look into the review. I don't believe we need to go as far as Steve Wright is suggesting in terms of sort of an optional menu of what's enforceable for different folks. I believe that we legally have and the regions legally have the discretion today to monitor and enforce whichever standards we feel suit an individual entity and that's really the purpose of the inherent risk assessment and really creating a risk profile for each entity.

And I think the regions could continue to do a better job of explaining that and explaining what will be looked at and I think there can be a negotiation between the entity, but I don't think it makes sense to take a North American set of standards and start creating sort of a little checklist matrix for each entity. The standards are the standards, but if you buy in a philosophy of the purpose of looking at anything is prevent the next failure it's going to point you to the ones that are important for that entity in that situation and based on their history and we

have full legal discretion to work on the ones that make sense.

CHAIRMAN LA FLEUR: But isn't it the concept of the standards that any of these things could be a leading indicator of something? You know because you don't know where the next failure is. You know the kind of pyramid of little things lead to big things. So is the concept that someone might find a company violating a standard, but say, well, that one isn't really like to contribute to an outage.

MR. CAULEY: Well, another concept of this pivot is really to get the entities to focus every day on the small things so that they're managing that. So the effective controls within a company to suppress the -- you've been saying this for years. It's a mountain of small things that can actually tip us over, but if we're fighting to suppress the small things on a day-to-day basis, the entities are involved in that, they're aware of that, we're monitoring the effectiveness of their internal controls monitoring. They're self-reporting. They're self-correcting. That helps deal with that sort of sneaking up through a bunch of small things.

CHAIRMAN LA FLEUR: Thank you.

I want to turn to a different hot topic and that's fuel and fuel security. Secretary Hoffman talked about it in talking about the 60-day study. I believe Gerry

talked about Aliso Canyon, which is something we're very closely watching, especially on a day when it's extremely hot in Southern California like today.

Back in -- I think it was 2012 when we first started on gas/electric and I put out like three questions or four questions, I don't remember, to the industry. One of them was how should we address this and one of them was is there something we should be doing with standards. And the immediate reaction was whatever you do this has nothing to do with standards. Don't do standards. But is there something now, as we look at the changes in the system and the decreased reliance on types of technologies that have on-site fuel as an exclusive base load. Should we be changing our planning standards in some way to take that potential loss of the pipeline into account or the gas storage? Is there something we should be doing in -- that NERC should be doing in that area around that issue?

I know there's a market aspect, but there might be a reliability requirement aspect. Something I know Gerry's hinted at for years, but I mean Aliso Canyon brings it, at least, into the front of topic. Excuse me; it was Secretary Hoffman who mentioned Aliso Canyon.

So I'm interested in if anyone thinks that our planning standards or something else should be changed because of the fuel situation we have now.

MR. CAULEY: I could take a first stab. So we're doing a special assessment project right now and I expect the report to be out -- I don't know the exact date, but 30 to 60 days its coming. And it's looking at critical points in that dependence between gas and electric where pipeline failures or we've gone around evaluated the different storage sites and looked at the potential impact of loss of key facilities. And philosophically, putting aside the question of a standard, it would be clear from this report, I believe, that you should be planning for the loss of a most critical, a most impactful facility, including if it's on a gas system

And so I think the answer is it may point to -- once we understand the issue, understand how significant it is, how many places does it occur; but it would be good practice to plan for that loss because you never know it won't happen.

I would go further and probably go out a little bit of a limb, but I think there's a general challenge that we need to step back at a policy level and look at the reliability, dependability, and security of the fuel delivery system on gas, given how dependent we are in so many regions. And I know we don't have any jurisdiction at all in the gas arena, but I know the Commission does.

CHAIRMAN LA FLEUR: Well, we don't have the

reliability jurisdiction over gas, but we have reliability jurisdiction over the people who burn the gas.

MR. CAULEY: Right. I'm not a lawyer, so I'm just making loose statements, as an engineer, but I am concerned that you have certain reliability expectations and standards on the electric system and what I consider a foundational piece, which is the fuel delivery doesn't have equivalent standards or expectations of dependency and reliability and security. I don't have a specific proposal, but I think that that's there to be looked, at in addition to your question, which is do we need to look at our planning and when it's one is now loss of a specific critical gas facility, which I agree with.

CHAIRMAN LA FLEUR: Thank you. Pat.

MS. HOFFMAN: So I look at it that the important thing that the regions and the grid operators need to do is an assessment of the fuel risks to grid operations. And so as looking at the level of regional diversity and to the extent possible how dependent is a region on one fuel source and from that perspective so that it gets to the point that Gerry brought up of really what is the risk to the reliability of the electric system.

But at the end of the day, I know the market operators are really looking at availability and saying that there has to be redundancy in fuel supplies and putting the

onus on the generators to make sure that they have fuel availability as part of providing electrons and electricity to the system and reliability to the system. So I think it can come down to that point of handling it from a redundancy point of view, but also, I think it's important to have a risk assessment done.

CHAIRMAN LA FLEUR: Thank you.

And I'll ask one more question and that's on data. I think it was John Hughes who talked about metrics, about the standards, and which have impact.

Reading the State of Reliability Report, it's obvious we have more and more data on elements of reliability, but the grid is yielding more data all the time with the PMUs and with the analytics that we're capable of with CADs and GADs and so forth. Is there more that we can do in the area of leading indicators of reliability issues with the new data that we have and should we be expanding our data collection? It's always a question of how do you balance using the data to get the lessons from it with protecting it because of the security, but it seems like its more of a data analytics world and I wonder if we're doing everything we can in this area or there's something the Commission should be doing.

MS. HOFFMAN: So I think data provides a great opportunity for improving the operations of the grid,

especially in assess management. I think from my perspective as you look into where some of the leading indicators are goes after, say, some of the data that's been helpful for transformer, looking at predictive failure and assessment management, so I think that's one are of opportunity.

I am concerned about security of the data, but the value of machine learning and being able to get more predictive in nature and looking probabilistic assessment I think really will provide value for the grid.

MR. CAULEY: So I think our ability to collect data from industry and their willingness to provide it to us and to be able to turn it into meaningful results and analysis is really one of the success stories we've had over the last five, six, seven years and I think it will continue. And it's really the foundation to everything we're doing. There are some areas where I believe there's probably going to need more, but we do want to be judicious with the burden and the security issues with having that data.

One thing I know we do need to get is some better clarity and granularity around reporting of security incidents because we have OA417 and we have EOP004 for reporting of incidents, sabotage reporting, and so on, but it's very sparse. And so the question is working with

industry what makes sense to create a sufficient set of data to analyze are the threats getting worse, are things happening more frequently, are the entities getting into our systems, deeper into our systems.

I also believe that we don't have -- NERC has really focused I think this coming year to come up with a better set of security metrics, understand security risks. The idea of, well, no cyber attack is going to cause a blackout. Well, that doesn't mean there won't be one tomorrow, so how do you measure risks, but you need data on the front end to make that happen.

Just to follow up on Pat's comment, I believe getting -- sort of corralling the value of PMU data for metrics is probably on our horizon in terms of understanding behavior system. I think you can see the behavior of the renewable inverters-based resources and distributed energy resources. The granularity of the PMU data is so fine that you'll be able to see the nuances of those measurements and try to get some leading indicators of problems I think through that approach.

CHAIRMAN LA FLEUR: Thank you. I appreciate your comment on burden and I hope we're looking at a future where we pass fewer rules where some busy person in a control room has to fill out one more report because I've been there and I know some times where that priority comes

in versus keeping the lights on and more situations where the actual equipment or the grid is giving us data without human intervention.

I guess let my colleague. Maybe she'll make some of the people I haven't bothered work. Thank you.

COMMISSIONER HONORABLE: Thank you, Cheryl. Good morning everyone and thank you for teeing up a really robust discussion. I'm like, Cheryl, I don't really know where to start, but I will pick up on the Aliso Canyon topic because I think this is an excellent example of the ability that we all have to play a role. And I think Secretary Hoffman mentioned the federal and regional responsibilities, but I also wanted to tee up because Chairman Haque, Chairman Twitty -- I like calling you that Chairman Twitty -- and John Hughes have also touched on this important need to coordinate the federal and state and local level -- that's a nod to folks, the LPPC folks -- but also, making sure we're playing well with our state colleagues and coordinating. I think there's an important role to play.

So while we've been very focused certainly on watching the Aliso Canyon Incident, I want to commend the Taskforce for working diligently on that, certainly, DOE for watching it and NERC's role as well. There's clearly a role for state regulators to play here and I think this Chairman Haque's point as well that states have lead in this area.

And this is an example of the importance of our state colleagues appreciating this issue we got passed last summer, thankfully. But according to the summer assessment, we have to be very cautious going forward, so I wanted to ask the Secretary and any others if they wanted to comment about either Aliso in particular or how we can do a better job of being mindful of our state colleagues' role, but also making room for them to continue leading here was well.

MS. HOFFMAN: So a couple of comments that I'd like to make as I was thinking about this and that there has to be coordination. As the states think about their investment strategy, whether it's generation, whether it's storage, I think there has to be a close coordination with the reliability coordinators in doing a system evaluation so we can stay ahead of the game of what potential investments are required, whether you take the polar vortex, whether take Aliso Canyon, whether you take the Northeast and the gas infrastructure issues.

I think from my perspective the interdependency play is going to be let's take a hard look at the policies, the infrastructures, whether it's battery storage or gas storage. There is some level of storage that is required on the system and think about what are the cost-effective solutions and what really can be optimized to the benefit of

the system. So having that close coordination with the states is absolutely critical.

MR. HAGUE: Well, thank you for the question Commissioner. This question gets more complicated when you start thinking about states that are in organized markets and states that are not. So it creates one grand, circuitous world of confusion when you start thinking about the State Subsidy Tech Conference that you held and it is an extraordinarily challenging issue.

I guess without getting to prescriptive, I have always thought that reliability should be the tie that binds. So in taking my NARUC hat off and putting my Ohio hat on, we have been through the arch of our now famous or infamous PPA cases. There were a tremendous number of policy considerations that were espoused in those cases. I think, though, that what has been missing from the dialogue broadly is the true on sort of reliability concept.

And so because of the market issue, the state that resides in an organized market or your typical cost-of-service state, I don't know that there's a silver bullet to this answer of utilizing whatever comes out of a reliability study to socialize that then across states and have some kind of uniform response, but at the very least, from a policy perspective, again, I do think that we are all on the same page with respect to that particular issue, so I

do think it can be helpful.

And I think that -- look, so I've been doing this now -- this is my fourth year doing this.

COMMISSIONER HONORABLE: Thank you, by the way, for doing it.

MR. HAQUE: Thank you. Again, thank you, I think to that, but thank you for the opportunity. And our state engagement -- the arch of state engagement has dramatically increased over this just four years. Initially, it was just about cost and now we're talking about this concept of base-load resources. We've been talking about that for a few years now and now we're talking about a totally changing even state rubric with all of the grid mode endeavors that you're seeing and how that will interact with the Bulk Power System. So I think you're right and I think we all recognize that. I think reliability is the tie that binds, but because of especially on the bulk side the markets issue it's an extraordinarily challenging issue, but at least on the distributed resources side I think there's some real opportunity there.

COMMISSIONER HONORABLE: Thank you. Anyone else, Chairman Twitty?

MR. TWITTY: Well, Commissioner, I appreciate you particularly pointing out that there is local authority as well. People used to say to me, well, you're not

regulated by anybody. No, you're regulated a local city council or a local board of public utilities or public works or whatever it's called. And I think the point I would make, and it also goes back to the data question a little bit, and that is just a real focus on the coordination of information flow.

Think about if there was an event on the system today you could have three or four or five different agencies requesting information and if you only have to provide it once that's a heck of a lot better than three or four or five. And the same thing about this, just remember that there are local regulators. Steve and I would both we would agree with that, whether it's LPPC or TAPS.

Those folks, again, they're the people, the store or church next Sunday that are going to button-hole you and wonder what in the world happened. And like Mr. O'Neil said once, you know the government that's closest to the people is the best, not to say bad things about FERC or NERC, but it is true.

COMMISSIONER HONORABLE: Thank you.

I wanted to turn now to just acknowledge the fine work of NERC and all of the stakeholders who participated in the supply chain matter. I wanted to say thank you for your effort. I know you worked so hard to get across that line, but I was very pleased to hear the report

that it got through in the second balloting.

And Gerry, I wanted to turn and ask you a couple of questions. One is to also commend -- I teed it up in my opening remarks -- the work of the entire sector on focusing on MISOPS, in particular. And it was really a beautiful thing to watch, to participate with you and your colleagues at the MRC and at the Board level, to engage with regionally, to even sit in, in an RTO meeting. I happened to be in Little Rock at the SPP meeting and heard a very robust discussion about the state of play with regard to MISOPS and what a number of folks across the industry sector were doing to focus on that and we've seen great results.

I also noted in your report that human error, of course, continues to be a challenge, to err is human, and I wanted to ask you what are the lessons that you've learned with your very deliberate approach to tackling MISOPS that you can also employ with human error matters?

MR. CAULEY: That's a great question. I appreciate the feedback. You know I think the story that we're still working on and it's unfolding and really miss operations is really a great example of the ERO should work, which is data points to a recurring theme of harms being done, outages being bigger than it should, load shedding and so on, and we say why is it telling us that. And the volume of data that we can see across North America really I think

is helpful compared to what each company could see because the company's been doing really miss operation analysis for decades, way before we were doing this.

But to be able to see the big picture and to see the pattern at a big level is really helpful. The solutions phrase has really been interesting because we've involved the North American Transmission Forum. Each of the eight regions has their own individual program, so it kind of gets customized and distributed out to get the work done. We're not pulling levers and managing the work.

The interesting piece is there are some entities that have rates high as 19, 18, 20 percent miss operations and some as low as 4 percent. Some of those are for reasonable, physical reasons why because the system design is different and different geographic areas, but it tells us that we can focus on particular regions or we can focus on particular entities and drive the performance to continue to be a lot better.

I think we can repeat that in the human error field with one concern, so that the solutions in relay miss operation space are very technical, so there's a series of loose connections, polarity reversed, the communications are not correct to coordinate between two relays that need to talk to each other. So the solution space in relays tend to be technical, mechanical, objective things you can do. And

once you fix them, they're kind of fixed. But if you can imagine now where I'm going with this, it's going to be a lot more different things can happen. You don't just fix one thing one time, so we're working, once again, with the Forum. We've done a joint workshop with them. We're doing peer reviews of best practices in human performance, but it's much more of a morphs transition. It's not fix one thing at a time. It's going to be building awareness, building best practices, building controls around that and I think we'll see a similar trend in human performance. It has gotten better in terms of impacts and I think we'll start seeing a sort of level of excellence in human performance in terms of error rates we'll be seeing in the coming years.

COMMISSIONER HONORABLE: Thank you. And I want to thank you and your colleagues and all stakeholders in advance because we know it's something that will occur, but I appreciate the focus on it because I'm certain there are certain areas that are common -- you know common human errors that can be focused on and I appreciate that you have already seen that and seen ways to improve it because the system is benefitting from it.

I wanted to touch on the Blue Cut wildfire incident because you mentioned the tripping of the two 500kv lines in the fire area and the loss of more than a thousand

megawatts across multiple areas and I wanted to ask you what did you learn from that and what can we employ going forward to be responsive to a situation such as that. And I'll also give Cheryl an opportunity if I didn't quite ask her question to jump in.

MR. CAULEY: I think we learned at different levels. You know at the highest level in terms of ERO role, once again, going back to the data having data and having -- this was not really a reportable event. It didn't actually make the news.

COMMISSIONER HONORABLE: And if I could say, that's why I was particularly interested in it, the fact that it wasn't a reportable incident.

MR. CAULEY: But we saw a series of frequency anomalies that day and we looked at why did that happen, but we had the data and we were able to work with Cal ISO and Southern Cal ISO and others to like let's investigate this even though it doesn't hit the criteria to require an investigation, but it's really interesting, and so we were able to do that, so one lesson is keep doing this.

I think with the introduction of DERs and renewables and inverters and new technology keep looking for anomalies that we don't understand why they're happening, keep digging.

I think we learned, as I mentioned, that the

standards talk about ride-through for generation. Once we investigated this event with the vendors, their understanding of ride-through had nothing to do with our understanding of ride-through. Our understanding of ride-through is you keep producing megawatts because if something's happening on the system around you, you don't want to like drop your production and increase through a cascade into further frequency. They thought ride-through was just shut off the power, but hang on there so they're connected, but they're not actually producing anything.

And we also learned that introduction of time horizons, and this is not just in wind and solar inverters, but this is in distributed energy resources and new relays that are coming in that a lot of this equipment is operating in microseconds and they're deciding and acting and doing things before the old, clunky, moving things have time to move or do anything, so that creates a whole new field of reliability concerns is how do we coordinate. The solution in this case is that the manufacturers are telling us, well, we can slow that down. We just didn't know you needed that, so we can put a five cycle delay or a second delay on something and let the system do what it's supposed to do before we decide what to do.

So I think there's a lot to learn and I think it's a field that's going to be at the forefront of

reliability for a long time.

CHAIRMAN LA FLEUR: I guess my question, and it was really a question that was provided by David Ortiz. I don't think I'm smart enough to think it. Is this an issue that's endemic to inverters generally that we need to watch for other places or was it just kind of growing pains on the assumptions and calculation frequency? So I mean how much do you think we need to look across to other situations versus just something that would sit there.

MR. CAULEY: Well, I think this is everywhere. This is basically, as we were thinking our strategy on how do we deal with new technologies, one thing we've realized is there's a whole lot of players now involved installing equipment on the system who probably many of them still don't know who NERC is, but certainly, they didn't know who NERC was a year or two ago. But they're putting equipment on a system at high volumes of resources and so they don't understand what the terminology means. They don't understand how we measure frequency and voltage and what the words in the standards mean because we do have a clear blueprint in the standards for how generators should behave when they're connected to the system.

Now we're miscommunicating because their understanding is at a level of electronics and the speed of their systems and this is a different level. So I think

it's widespread.

One of the things I wanted to do is make sure we get this quick enough that we don't get into regrettable situations in terms of installation of new facilities. And we're still investigating, but the vendors have told us that 40 percent of the inverters that were involved in the Blue Cut incident cannot be corrected for the voltage problem. So that means they're producers. They can produce megawatts. They can be there. The can be planned for, but if there's a disturbance you have to assume that 40 percent of that generation will leave.

So what we want to do is get the work done urgently enough that we don't have any more facilities installed that don't have the capability to operate and it's expensive to replace them once they're in.

CHAIRMAN LA FLEUR: Needless to say, when I've talked to solar industry groups and wind industry groups, I frequently urge them to get more involved with NERC, so I'll use the bully pulpit here. It's really essential.

COMMISSIONER HONORABLE: I, too, think Gerry your comments speak to not only flexibility, but inoperability and just reminds me of when I was chairman of Arkansas Public Service Commission and we would have a mayor who was gung-ho about putting a wind tower up, but had no clue of -- some vendor came and said, no, put the wind power

up and then go to the Commission. You know he didn't know he needed to come to the Commission and the fact that he didn't come first caused a whole world of problems for him.

And to your point, our ability to master how we're working with integrating these inverters in such an credibly wonderful time with greater amounts of renewables, but our ability to harness that in a way that still gives us -- I think Pat spoke to being nimble and flexible -- still allowing us to do that. So thank you. I wanted to ask your lessons learned.

I wanted to turn to both, Charles King and Mr. Wright, because you both, in your comments, teed up a discussion I wanted to have. One is I too want to commend the industry broadly, and when I say "industry," all stakeholders, but yes, industry meaning EEI as well for your leadership in the ways in which you continue to work.

I agree with you that, yes, we need standards, but that there are number of ways in which industry, collectively, the sector, is working in ways -- I love the way you said it -- to supplement this important work. So it's a great time for us to reflect upon now 10 years of mandatory reliability standards, but it's great to talk about the ESCC work, the work happening at the ISAC with the ISAC effort, with fusion centers, with all of the ways in which we're working together. And I'm very pleased that

you mentioned mutual assistance, the spare transformer efforts. So I wanted to take this moment to thank you and your colleagues at EEI for your leadership there.

Mr. Wright, you raised an interesting point about the fact that, in your opinion -- and I wanted to ask you to talk more about this. You think that we may need to create more incentive or did I write "rewards" or did you say "rewards" for compliance? This is an interesting discussion in my mind because I have a 16-year-old and she gets good grades, but I think she could get better grade. So do I reward her for -- you know where I'm headed with this -- for getting the grades she should be getting anyway.

MR. WRIGHT: I have a 17-year-old son, so I'm right with you on this one.

COMMISSIONER HONORABLE: So we're speaking the same language. I want to ask you to elaborate on that because I think even in the context of our work here at FERC we have heard some stakeholders saying this is the work we should be doing. This is our job. But I want you to talk more about using this carrot approach versus the stick approach. I think for us in the U.S., I think we've seen it work particularly well, so I wanted to invite you to talk more about that.

MR. WRIGHT: Well, I think this is a little bit of the conversation we were having earlier too. I want to

spend some more time with Gerry because I heard him say that there is a way to work with the regions that maybe has not been fully exercised yet and I'd like to understand that better because I think one of the things that has happened is the whole commitment to the RAI Program has caused utilities to go down this path of doing really elaborate inherent risk assessment and internal controls evaluations work. And I just say from my experience that has been really good work. We've learned a lot of things that we didn't know about the way our systems operate.

We've learned about the way our system impacts the Bulk-Electric System that we didn't know and probably should've known, so there's been some really valuable things that have happened there. There should be an opportunity as well to be able to learn there are places on our system that have a big impact and we need to really be focused and there places on our system that don't have a big impact how can address that in terms of trying to wring some efficiencies out the system. I think that's the challenge that we face.

COMMISSIONER HONORABLE: And really take a risk-based approach.

MR. WRIGHT: That's right. So that had been, at least from my understanding when we first started down this path three, four years, were I said we were going to go out and we were going to learn a bunch about where it is that

individual systems and eve facilities within systems were really critical to the system and were they were not and that we would be able to advance our protection of the system through that knowledge that we would gain.

And so we're now to that point where we've gained a lot of knowledge. Now the question is how are we going to exercise that knowledge to be able to take advantage of it. And again, we're spending a lot of money on this. I think it's a good thing because we're improving reliability, but if we can find efficiencies, we should go find them and try to get them.

COMMISSIONER HONORABLE: Thank you. Any others want to comment on that point?

I, too, appreciate Mr. Wright that you mentioned opportunity at the regional level.

To Chairman Hague's point, I think that could open up another level of complexity. I think we continue to have discussions about the best regional approaches and ways to get regional efficiency in the context of enforcing mandatory reliability standards, but also harnessing greater efficiencies in our day-to-day reliability work. So thank you for mentioning that and I look forward to greater discussion about the best ways to do that going forward. And thank you all for appearing here today.

MR. BARDEE: Thank you, Commissioner. I think

staff we'll keep our questions to a minimum so that we don't get too far off schedule. I'll just ask one at this point and it's actually something that you might be able to address, Pat. Others are welcome to also, but it goes to the supply chain issue.

As you know, we required NERC to develop a standard. There's a standard in the process. It just passed its second ballot. Presumably, it'll come to us sometime later this year. And if we ever a quorum again, we'll do something with it, but at best, that is a solution that deals with a small part of a very big supply chain. It may reduce the risk for the entities subject to it that apply it, but the supply chain itself involve so many sectors and so many other aspects that are far beyond our role and I was wondering if there are efforts or things that DUE in conjunction with perhaps other parts of the government would be able to or is considering doing that could address parts that we can't.

MS. HOFFMAN: So thank you. That's a really important question and it's quite a complicated subject, as you talked about supply chain encompasses more of the subcomponents and parts and pieces than what was directly reflected upon in the standard. So some of the things that the industry should think about is trust in manufacturing and looking into assessment of the manufacturing process.

One of the things that the Department's looking at and considering is how do we further do testing and system testing of supply chain components so that we actually can have feedback to the industry from a risk assessment point of view. At the end of the day, it's going to have to be a collaborative process where industry understands the risks that are being posed by the supply chain components and their subcomponents, but also it has to be some disclosure of where some of those vulnerabilities may be. So we're going to look at some system testing, but we're also thinking about how do we learn some lessons from DoD from a trust in manufacturing point of view.

MR. HEGERLE: So let's try to tie together several things. I liked Gerry statement on fearlessly focusing on preventing the next outage. And Acting Chairman LaFleur mentioned data and metrics and others of you of the panelists mentioned that as well and Commissioner Honorable mentioned the learning that we could get from the MISOPS as applied to human error.

I was wondering about how well we can look at the interdependencies of these various data pieces to do that prevention in that when we look at averages we don't end up necessarily seeing the picture in a specific region or with specific entities that are close together and many of the outages that we've seen like the one five years ago

out West was one where one small mistake preventable was made by one entity, another was set up differently and a third and we have a problem. Is there a way? Can we, do we look at the interdependencies of those various pieces at a more macro -- not an individual entity, but a smaller, maybe a BA-area way of thinking about that or identifying those risks so that we can prevent, as Gerry was suggesting, those bigger events?

MR. CAULEY: Well, if I could call up Dr. James Merlow from the audience here, he could probably help me answer this better, but we are not focused simply on using averages or broad pictures, but we have some very good PhDs and statisticians on our staff that are looking for the patterns that are hidden in the noise and some of it I would call it sort of transactional or sort event drive. So you look for an event and you try to figure everything out and others are just sort a broad collection of data over time.

I think the one opportunity we could probably explore a little bit more is the interdependencies between the datasets. Now we do that to some extent now like if there's an event we're looking at the transmission performance through the TAPS database and we're looking at the generator performance through the gas database and saying well why did they all combine to leave. So we are doing some cross-dependency, but I think the error you're

talking about I think is a new opportunity maybe. Even when there's no event and it's a sort of a blue sky day, are there any correlations between data and across the databases. I think that's an interesting question. We'll talk about it when we get home.

MS. HOFFMAN: If I may add one thing. I think the value of the PMU data is a dataset that's consistent across the whole industry that provides a platform where grid operators can look at consistent tools and actually be able to do forensics and analysis and asset management. So moving forward, we need to have a similar set of platforms of data, whether it's sensor-based data, the distribution system that the industry writ large can build upon for visibility and really speed up some of the understandings of what's happening and that has to be paired appropriately with the data that's feed into modeling and analysis of the system

MR. BARDEE: So with that, I think we'll conclude our first panel. I'd like to thank all of you for your time today and we really appreciate it.

MR. WRIGHT: Mr. Bardee, can I make just one quick comment, if I could? I'd appreciate it.

I did participate in the first one of these conferences way back in -- I think it was 2010. And there was a lot of tension in the industry at that point and there

was one of the reasons for this conference. And I just want to say back I think at the second conference I made a recommendation that this be formalized and happen more frequently and I want to say right now that that was unnecessary. And the reason it as unnecessary is because of the way folks have chosen to participate in processes since then. So Gerry has run his organization in a very transparent way that made it not necessary to do this.

The FERC staff has been much more open, I think, in terms of engaging with the industry and the Commissioners have gone to the MRC meetings. So for really good reasons collaboration has occurred and I just want to say that has made this law work a lot better and I appreciate it.

MR. BARDEE: Thank you. Thanks again.

So if our next set of panelists could please come to the table.

Alright, we're going to start our second panel now.

COMMISSIONER HONORABLE: Mr. Bardee, if you don't mind, I'm going to raise my voice a little bit. Ladies and gentlemen, I love that you're enjoying this so much, but we are going to proceed to our next panel. Thank you so much for your attention.

MR. BARDEE: That's why she's a Commissioner and I'm just a staffer. So let's start our second panel here

with speakers from other parts of the world, not the United States and it's an opportunity for us to hear what's happening in other countries, North America and Europe, and to learn what we can that may help us and share our experiences. So I will start by introducing Mr. Brian Hewson from the Ontario Energy Board.

STATEMENT OF MR. BRIAN HEWSON

MR. HEWSON: Acting Chair LaFleur, Commissioner Honorable, staff, and my fellow panelists, good morning and thank you for the opportunity to come and speak today. My name is Brian Hewson. I am the Vice President of Consumer Protection and Industry Performance at the Ontario Energy Board, which is the gas and electric regulator in the province of Ontario in Canada.

And while I will touch briefly on some matters of all of Canada, my remarks will generally focus largely on Ontario because that is where I'm most knowledgeable and most experienced. And I think the experience that we've had in Ontario will touch very closely on a number of the questions that were asked in your agenda.

Canada and the U.S. are a highly integrated electricity network system. As you will know I'm sure, there are 34 interconnections between U.S. states and Canada. There's also 33 major inter-prevental connections, which makes inter-ties a very important part of the

operation of our grid in Ontario and a very important part of the operation any considerations of the OEB.

As you know, unlike FERC, in Canada each of the provinces and territories are responsible for reliability oversight of the transmission network. You know following the 2003 blackout, the federal and provincial ministers of energy got together and decided that there should be a close cooperation and coordination across the country and they've established a working group, which we are a fully active member of, that coordinates and discusses both activities in relation to NERC and activities across the country in terms of coordination and ensuring reliability.

Each Canadian jurisdiction has implemented its own approach to ensuring that reliability of the local electricity system is taken care of. Each enforces NERC compliance through a variety of models. In Ontario, I'll speak to specifically, our independent electricity system operator is the designated entity that's in charge of ensuring reliability of the system and monitors and enforces the reliability standards enforced by NERC with the Ontario Energy Board as its backdoor or backstop, I should say. We are there to make sure that if someone needs to have further sanctions against them, we are in the position to do that.

You know your questions really focused us on the issue of renewable and distributed generator and how Canada,

and in my case, Ontario is managing the evolutionary change. What I can tell you is that the provinces of Canada are heavily involved in renewable energy. As you will have seen in my notes that I've provided, roughly, two-thirds of the electricity that is provided in Canada is produced through renewable sources. And that includes the provinces of Newfoundland, Quebec, BC, Manitoba, and Yukon where they rely on almost 95 percent of their electricity is produced through hydroelectric facilities.

Ontario -- now I'm going to focus a little more closely on Ontario -- has gone through a significant supply change over the last 10 years. By 2025, our IESO is forecasting we will have renewable resources connected at both the transmission distribution level that nearly make up 50 percent of installed generation. The bulk of the rest of our generation is nuclear and we are in the process of a major refurbishment of all of our existing nuclear units to be able to continue their operation.

We did change and increased the renewables as part of a government desire to eliminate coal as part of the Ontario supply mix. While we were eliminating coal, we recognized that we were bring on intermittent renewables and that that required changes to our market rules to make sure that intermittents were playing their proper role within the IESO grid and IESO markets as well as investments in

upgrades to both transmission systems and distribution systems.

At this point much of Ontario is looking at approximately by the end of this year having over 3600 megawatts of distributed generation. That compares to the mid-2000 when we had under 100 megawatts of generation that was connected to the distributors. That distributed generation is causing many changes in our system. We have facilitated the change through rules to require nondiscriminatory access by distributed generation. We've imposed contract requirements that ensure that connection processes are timely, but respect reliability and security requirements. We've also implemented changes to rules to facility good public policy.

On the gas side, I did hear mentioned we have recognized the importance because of the increase in gas generation to be assured that there is good coordination, so the IESO has been required to develop a coordination taskforce with the gas distributors and gas generators. As well, they have implemented a new grid, LDC, Local Distribution Coordination, Committee to ensure that there is greater task connection and data sharing across the two entities.

They've also focused on frequency regulation, voltage control, and flexibility increases.

In closing, I'd like to say that the provinces and territories in Canada will maintain our collective and collaborative efforts to ensure that successful outcomes continue to be achieved as the supply situation changes and evolves. As the first jurisdiction in North America to implement mandatory NERC standards, Ontario plans to continue to play a key and leading role in that collaborative effort.

I thank the Commission and look forward to any questions.

MR. BARDEE: Thank you, Mr. Hewson. Next, we have Commissioner Madrigal from CRE in Mexico.

STATEMENT OF COMMISSIONER MARCELION MADRIGAL

COMMISSIONER MADRIGAL: Thank you very much, Chairman LaFleur, Commissioner Honorable, colleagues, we think a lot of your invitation to speak on behalf of the Regulatory Commission in Mexico. We believe sharing experiences is very important. WE have learned a lot from our neighbors in the process of implementing this tremendous energy reform and I will speak in my remarks about the reliability issues with regard to integration of renewable, distributed generation and some of the issues that we are seeing in the gas markets, so I really thank you for the opportunity to be here.

Most of my comments will be, of course, personal

comments. When there are Commission decisions, I will clearly state those aspects. So with perfect ongoing energy reform in Mexico, renewables will increase up to 35 percent by 2024. Right now clean energy sources in Mexico are about 20 percent. In our legislation, clean also means large hydro, including nuclear. We have a large nuclear power station. So out of those roughly 40 percent of -- renewable resources, mainly, wind and solar, but with the recent success of the energy options, we may reach 10 percent of whatever renewable resources just in a question of one or two years.

Why? Because we have contracted roughly 6 g-watts of new capacity to be added in the next two years, mainly, solar because of the attractive prices we are getting in the market. So what we have been contracted recently is more than what the system has added in the past eight to ten years. So we are going to see a very rapid increase of valuable resources in the next two to three years, reaching up to 10 percent of valuable resources.

In the distributed generation, solar is growing exponentially. Roughly, 40 years ago, we had zero installations at the distributed level, now we have 29,000 installations. Roughly, they make up for 250 megawatts and the size of the installations are growing from an average 5 kilowatt to 10 kilowatt. The Commission has issued rules to

continue with distributed generation. We have three streams -- net-metering, net-building, and wholesale of distributed generation to the spot market now that it is facilitated with the energy reform. So we continue using net-metering as a way to facilitate consumers engagement with the market. Of course, those mechanisms will evolve. The new rules have a sunset clause. We will review those, but we believe this is an efficient way to make consumers ready to engage in these activities.

The grid code level we're incorporating some smart and better features into our distributed generation rules so our control center in Mexico is gaining expediency on managing renewables. As part of the new market rules, all renewable suppliers have to provide forecast to the -- . This is the control center. They improve that forecast. And in the last issue transmission investment plans in assay is really looking ahead on what investments are required for the suns that is more investment in solar power. So proactive planning to make sure transmission reaches those areas in a reliable way.

As part of the reform, we create in Mexico it's like FERC, NERC, and the state regulated altogether, so we have the responsibility to look after wholesale, retail rates, reliability at the federal level, so we issued the first independently release grid code, which is more the

reliability standards as a whole, include planning, operations, and interconnection requirements. We are using the expedience worldwide in terms of making sure we have technologies that cooperate with the grid. We are in the process of preparing the first annual, independently issued reliability report and we will see what happens and what revisions in the first version of that reliability report.

On the gas side, as you know, natural gas is very important for us. We rely a lot of imports from gas from the U.S. as 55 percent of our gas supply comes from the U.S. and makes for probably 40 percent of our electricity mix. We're also in the process of creating a gas market in Mexico. At the Commission last week we basically freed the previously regulated wholesale price of gas. We're in the process of building a market and in that process there is also an independent system operator of the gas market recently created with the energy reform. Its name is Senegas. And Senegas now that our market is evolving in gas it is also in the process of writing the first grid code for operating the gas infrastructure of the country. There we have jurisdiction. We approve the rules for the gas system operator, so we are in the process with technical groups to write that code.

Of course, any reliability issues in the gas sector has big implication for the power grid in Mexico and

in the expansion plans of the power sector. The Commission has issued comments that this interaction should be looked after more carefully from the planning perspective, so we have been able to manage issues with gas supply mainly through demand production programs and we continue to work in that.

Now looking ahead, the Ministry of Energy, which is the policymaker in Mexico, is in the process of drafting a gas security supply policy, looking at possibly storage quotas. We don't have a policy yet. A policy is under consultation for the fuels market and we already have a policy on the security of supply for the power grid.

So that was basically my general comments and I look forward for a deeper discussion. Thank you.

MR. BARDEE: Thank you, Commission. And finally, we have Klaus Dieter Borchardt, Director for Energy at the European Commission.

STATEMENT OF MR. KLAUS DIETER BORCHARDT

MR. BORCHARDT: Thank you very much, Mike, Acting Chairman LaFleur, Commissioner Honorable.

First of all, I'm very happy to be here again and that FERC has invited me again to this conference here. It's a real honor for me to be allowed to present the European view in this panel.

As you all might know that the European energy

system is already in the middle of profound change. All had started about 20 years where we had broken up the structures of the more than nationalized energy markets by unbundling the by then integrated, vertically integrated companies and unbundling them from production and supply and transmission. That was the first important step.

The second step in these changes were the creation and the development of network codes and guidelines, a bit similar of what I've just heard here from my Mexican colleague. This work we have nine network codes and guidelines. This work has been finished recently in March this year with balancing code in electricity. And now we are just entering in the next phase and this phase has very much to do with what I call flexibility.

Why is that so? The European system, of course, is based on a new climate policy to which the European Union is heavily committed. We have initially started by giving ourselves legally-binding targets. They are running of 2020 was minus 20 percent CO2 emissions, 20 percent share of renewables, and 20 percent energy efficiency. And now within COP21 and Paris Agreement Complex, we have globalize new commitments time horizon 2030, minus 40 percent CO2 emissions, at least 27 percent share of renewables in the system, and 30 percent energy efficiency.

And when you look at, at least 27 percent, this

is necessary in order to make it up to the 40 percent CO2 emissions because 60 percent of the emissions are coming from the energy system. And 27 percent means not less than 50 percent of the whole electricity consumption use, have to come from renewables and here intermittent renewables, solar and onshore winds, but offshore winds coming very strongly.

So this, of course, creates huge challenges for our energy markets, but not only the markets, as I've said, for us the drivers for reaching our climate goals are energy efficiency, so therefore we have proposed a profound reform here as well, and renewables. And this, of course, now has to relate to the market. And what we can see is that the market, as it stands now, is not up to the challenges.

We have not enough flexibility in the market, neither on the generation side, nor on the demand side and this is, of course, of paramount importance because we still firmly believe that a well-functioning market is the most cost efficient way to deliver electricity to the consumers. So therefore we have put forward as a Commission a very comprehensive package, not less than eight legal acts comprising in a clean energy for all European package and it's free of these concerning the market design of the electricity market.

And I would like just to focus on the four building blocks of this market design, part of this package.

The first building block are the consumers and here we are trying to put the consumers into the center of our energy system and trying to make them participate in the development of our energy system.

And I will only highlight two concrete measures here. The first is that we give them an unconditioned right, all consumers, individually or collectively, in energy communities to produce, to store, and to sell energy. The second is the demand side response. Here we foresee two different ways. One is price driven. Here we provide the consumers with dynamic pricing systems and smart meters so that they can adapt a consumption to the price situation and the other is incentive-based. Here we are creating a very robust legal framework for aggregators so that they can enter into the market and do this demand side management.

On the wholesale market, of course, it is the integration of the intermittent renewables that we have and here it's very clear that we are moving away from base-load capacity to flexibility. Our intermittent renewables are not reconcilable with purely base-load capacity approach. How do we do that? First, we have to make the market fit for the renewables and that means in the first place we have to reform our balancing markets. We need much, much more balancing reserves and we need, of course, services at very short notice from generators and from the demand side

response in order to keep the system balanced in real time.

Here we are moving the balancing from the national to the regional level, so the calculation and also the procurement will not be done within the realms of the member state, but in the region. We are also finalizing our work on the short-term markets, which will become even more important in the future. So intra-day and day-ahead market coupling is about to be finalized.

Another issue is the pricing system. We are proposing that the price setting should only be done according to the market signals, nothing else. So that means that the old price caps and the regulated prices that you see in a number of systems in different members states -- 17 members states still have regulated prices -- have to be abolished and we've proposed that. We also want to allow prices to rise to the value of lost load in order to also reflect scarcity, so scarcity pricing has to come.

Another issue you know in Europe we are following the sonar pricing approach. The configuration of price zones is also an issue. The problem we have today is that the price zones are not designed where the congestion is, but under political considerations and it's political borders that are prevailing over the economic and technical ones and that we are changing as well.

We are introducing capacity mechanisms, but only

as a last resort instrument, capacity mechanisms that have to be proven its necessity at regional levels. So the adequacy assessment has to be done at regional level, not any more at national level. It has to be cross-border open so that can also companies from -- and other member states can participate in that end. Here we have introduced as well an emission performance standard, 550 grams CO2 per kilowatt hours, which will kick out or not allow in coal-fire power plants and some even gas-powered power plants. That's what we are doing on the market side.

On the renewable side, here we are bringing all of the renewable producers under the same obligations as any other generators, so that means balancing responsibilities, no priority dispatch any more. Another very important is because if you have more renewables you have decarbonized generation and you have closed integration. What does that mean for the interoperability? That means that we'll have much, much more interrelated system operations.

And in order to cope with that, we want to create the so-called regional operational centers. Here we have an organized cooperation between the respective TSOs in the regions and this ROX as we call them, they will at regional level do the sizing of the balancing reserves. They will do the capacity calculation. They will care about security and safety issues and they will also do their

generation adequacy.

The third building block is infrastructure. And here I can say that we have a well-working planning system in place with a 10-year network development plan, with a project of common interest, and to connect a newer facility bridging financing gaps, so this is all working well. But what we need more is very strong cooperation between DSOs and TSOs because in Europe the renewables to 60 to 90 percent are going directly into the distribution grid and they cannot cope with that alone, so there has to be very, very close planning and managing cooperation between DSOs and TSOs and we are putting the respective rules in place by creating a platform on which DSOs and TSOs have to carry out specific tasks.

And then, finally, digitalization as the building block. Here I have to say that our proposal currently in discussions in the Parliament and in the Council of Ministers has only some elements of digitalization like smart grids and smart meters innovation, how to bring more innovation into the energy system. But I think in future, and this is maybe a new challenge, more has to be done. We have to think about to use block chain here in order to make possible to be peer selling. I have heard in the previous discussion. I think you, Acting LaFleur, have mentioned that we need in real time information from

the grid, so you could also use this new databases to give us automatically without intervention of human beings this information. This is absolutely important. Also, the automation of the houses so what happens behind the meter will be an issue. We have not addressed it yet.

And last, but not least, also cybersecurity. My colleagues have mentioned gas. Gas is not part of this package. We are concentrating on the electricity side. We have a well-functioning gas market. Gas in this new system, in my view, will stay as a backup. We will go out of coal. Some member states will continue with nuclear, traditionally. We might have one member state staying in coal. That's forgiven, but mainly there is gas to stay as a backup.

So all-in-all, I must say that we have now a 1,000-page legal work on the legislators' table. We hope that we can get it through because without the changes that I have just mentioned briefly it will not be possible to live up to our commitments. Thank you very much.

MR. BARDEE: Thank you, Klaus. Commissioner Honorable, questions?

COMMISSIONER HONORABLE: Thank you, Mike. And I want to welcome our guests here and please know we are delighted to have you as part of our annual reliability tech conference. For our European colleagues, thank you Dr.

Dieter-Borchardt for continuing to grace us with your presence and we've learned so much from one another. And we were very pleased to host the European Commission here at FERC. I believe it was last year and we executed an MOU and we are honored to work with you.

And to our North American friends, I want to welcome you back as well, and particularly, you Commissioner Madrigal. And we have enjoyed cheering on our colleagues in Mexico and we talked about this quite a bit in our last annual reliability tech conference. And in fact, we moved this session up because we don't want you to be the end of the day because it's important, our work together. We've really been very pleased with all of the work occurring in Mexico with your ambitious energy reform, with standing up the grid code. We cheered you own when you got through your auctions and now to watch as you are standing up your gas grid code and market. We know that we are interconnected.

And I say the same thing to our Canadian colleague. I mentioned to Mr. Hewson before we started that I was just in Vancouver at the CAMPUT meeting. We were there together. And we are also interconnected in our work, both on the electric and gas side. And I'm particularly interested in the work in Canada in developing your carbon pricing scheme. I developed an international mentoring

program for women in the regulatory sector. And Rachel Levine is, or was, my mentee, so I learned a great deal, I know you know her, and learned a great deal from you all and I wish you well with that effort.

In the interest of time because I had a previously scheduled commitment, I will ask you one question and Chairman LaFleur is kind enough to ask my other question.

So I wanted to focus on our North American colleagues first. You both have talked about the dynamic shift in the energy mix and in particular the role that gas is playing. I wanted to ask you to talk with us about your gas/electric coordination efforts.

In particular, Mr. Hewson, I know you mentioned the IESO Taskforce and the grid LDC Coordinating Committee. Will you talk a little bit more about that? What is the mission or goal of each? How do they work together? And then I wanted to ask the same thing of the Commissioner? Thank you.

MR. HEWSON: Yes, thank you for the question. So first touching on the Gas and Electricity Integration Taskforce, back in about 2005 or so, as we saw the increase in natural gas as part of the electricity infrastructure, we actually held a proceeding to look at how to better ensure there was integration between electricity and the natural

gas systems.

Out of that, we focused on -- our rule was to focus on issues around transportation, gas rules, and storage gas rules and we implemented an actual first-of-kind in Canada what's called the Storage Access Rule, which defined particular considerations around more intermittent or required services like gas.

While we were doing that, our IESO actually decided that it should build a stronger relationship with the gas distributors in Ontario, who operate all of the high-pressure transmission system and deliver gas to all of the different gas generators, so they've had that Taskforce for probably about seven or eight years and it meets on a regular basis. And what they do is they share information between the distributors and the IESO to ensure that IESO is building in any planning issues related to the gas distribution system, upgrades to the transmission system and consideration in terms of its forecast for how the gas generators are going to be used.

As we've moved off coal, brought in more renewables, the gas generation system has obviously taken on a much greater role in terms of both reliability and meeting peak demand and so there's been a lot more work there. The LEC grid coordination work is something that the IESO started just a few months -- well, maybe not even a year

ago. After having conducted a few pilots with different utilities, learning about distributed generation and other distributed resources like storage were impacting on the distributor in flowing up into the system, they decided that they should actually form a union with the -- we have 70 distributors in Ontario, some very small, a few somewhat large, but they organized this so that they could start building a dataset and better mechanism for sharing information back and forth.

They have imposed requirements on large renewables that are embedded distributors to actually start providing reporting now and have done so for some time, but they're now looking at the next level down below 500kwu. They're looking to get deeper and deeper into the system.

COMMISSIONER MADRIGAL: Thanks Commissioner. Yes, in Mexico, the growing investments in the gas infrastructure are driven by the power utility, so from the beginning there is some sort of coordination.

Now formally, at the planning level, we, at the Commission, issue recommendations of both the transmission, the power electricity plan and the gas pipeline plant since we also approve the rates for the nation electricity grid and the national pipeline, so I see the Commission as being the facilitator of making sure the plants are efficient for both systems together. So we have issued comments of making

sure gas and electricity coordination is conducted well, especially in some areas where there may be competition between gas pipelines and electricity infrastructure. We have the ability to do that from the Commission.

At the operational level, there are actually already some rules to manage gas alerts. You know in Mexico demand still grows 3 to 4 percent and I think this year it's going to be a record hit of almost 5 percent, so our issues with gas were alerts. We consume all the gas we get and four years ago we had some alerts on gas availability or because of pipeline issues, so the power utility was able to manage those alerts by voluntarily demand reductions.

Now moving to a market, those rules to manage alerts have to be written in a way that are transparent to everyone, so as part of the market operational rules because we still have the issue of gas availability as some point we may have, so we wrote those rules to manage gas alerts.

Going forward, as I said, we're working with the gas system operator now to provide the gas operating rules or the grid code for gas system. So I think our ability to see what is happening in both sectors comes from the fact that both systems are a federal issue in Mexico. We see absolutely everything -- gas, electricity and we have the authority to approve rates and to comment on the investment plan. So the systems are growing and interconnected. There

are many things to be done still, but I think it's systems that basically have grown side-by-side and we're just hoping to continue like that.

Gas is very important for us, although we don't have a lot of availability issues, in the areas where we have lots of wind power, hydro, and gas combined cycle plants have been key to respond to some variation issues locally because of some transmission congestion, so we see that gas will continue to be a clean, cheap fuel for the transition, but we're actually phasing out the companies, some fossil fuel burning because of gas prices. So it happens to be a win/win. Gas will help with reliability and is helping lowering electricity prices.

COMMISSIONER HONORABLE: Thank you both and we'll continue to work well together; I'm certain of that. And please know that you're all welcome here any time. Thank you.

CHAIRMAN LA FLEUR: Thank you Collette. I'm going to start by asking Dr. Dieter-Borchardt one of Collette's questions, but I'll make it the first person plural, I think.

We, too, think that we need a greater flexibility in our markets to respond to the dynamic shift in energy production and consumption. And her question was what lessons learned can the European Commission share with

us as you've focused on this issue of managing the dynamic supply and consumption.

And I'm particularly interested -- this me speaking now -- in doing it with very little reliance on natural gas, which seems to be the go-to fuel to balance variable solar generation here in the United States in many places. So I'm very interested in your experience there, and then I'll ask your colleagues if they'd like to chime in anything.

DR. DIETER-BORCHARDT: I think to have the full answer you'll have invite me again once we are there because we are now really in the transition towards the system. For the moment, we have a clear base-load driven system that does not differ so much.

We have the particularity in Europe that each member state can decide on its own energy mix, which makes our life, when you have to bring all these together at the European, not easier.

CHAIRMAN LA FLEUR: We have much the same in many parts of the United States.

DR. DIETER-BORCHARDT: So then you know what I'm talking about. But anyway, what we are seeing is clearly that flexibility on the generation side what will that mean. I mean we will clearly go in Europe for very, very high share of renewables and mainly intermittent renewables in

future. It will be, as I said, solar, onshore, and more and more coming offshore wind and then you have some niche products. I'm not talking about that.

So that will be the mainstream of our generation. And in future it will be, in my view, backed up mainly by very, very flexible power plant, CCGTs. There you are coming back to gas and here you have the combination coming back to the first question. It is not in Europe without criticism because our problem with natural gas is that we are dependent on imports, more than 50 percent we have to import and our suppliers -- not all our suppliers are the most suitable one.

I would say for business that is not policy driven or even geopolitically driven, and I think you know what I mean, but in my view, the role, if I come back to the question before how we combine electricity and gas is more that we try to develop technologies that are economically viable to transform power to gas and using this. That's one of the fields where we come together.

On the pure flexibility, as I said, generation it will be highly intermittent renewables backed up with, in my view, nuclear and this flexible gas-fire power plant. If there's other power plants that have the same flexibility and we had discussions recently in China. The Chinese they are working on very flexible coal-fired power plants where

they can even meet our emission performance standard, they say. Then of course, that could be an option for those countries that are staying within.

On the other side, on the demand side, the flexibility here we see in Europe huge potential. If you look at it, currently, we are only taking in 21 gigawatt on demand side management. If we implement our proposals on demand side management price-based and incentive-based, we can go in 2030 to 160 gigawatt, so there is a huge potential also on that side really to bring this flexibility to the market.

CHAIRMAN LA FLEUR: I'd like to ask Mr. Hewson and Commissioner Madrigal if you'd like to chime in anything on that question or I'll move on.

COMMISSIONER MADRIGAL: What I think has been interesting for us is the discussion of when and what solutions do you need now for your level of penetration. What we're seeing in Mexico is that we could reach 10 percent of variables so quickly, like in one to two years, that we need to know what we need to do faster than, for example, -- in Europe, so not all countries can reach higher levels of penetration faster, so we need to implement the solutions faster. On that we're just learning from experience and learning from you, from Europe. And looking ahead, we're actually collaborating with -- to perform a

North American integration study to see what would be the solution for higher levels of penetration.

We do have some issues in an isolated area of the country -- very small, 200 megawatt system that is insulation. We set up a limit in that region and the limit was reached almost at the moment the rule was issued because it's so attractive solar power in those parts of the country, so we're working with the utility on reviewing if that limit is consistent or not with the practices we know you can implement already. So the issue of when and how fast you need to implement solutions is becoming an issue for us because we can do it faster, so what solutions do we need to put into table faster so we're learning from doing.

MR. HEWSON: I think all I would add is that as we implemented our coal phase out we did turn to gas. We have very good gas assets in the province and had always had a history of gas plants as one of the key sources. So we've put resources in place. What the government has committed us to look to do is to work with the distributors, the transmitters, the generators and mostly with the demand management community to work to make sure that we don't need to build any more plants.

So we're now in the province much more focused on a DR auction that is going very well. Our smarter pricing we've rolled in smart meters across the entire

province, implemented time-of-use pricing and we're now looking at models that would make even more dynamic pricing models put in place. So we've really got to the point where we're saying we're not going to -- we don't forecast needing to build new gas plants. What we're looking at is making sure that we keep up with the renewables.

CHAIRMAN LA FLEUR: Thank you.

It's really quite striking listening to all of you because you're going through a lot of the same challenges that we are and the same phenomena of transformation, although at a different pace and with national goals, whereas we're coping with the additional dimension of having different climate goals in a lot of the different states, which is an interesting feature right now.

I wanted to also ask Dr. Dieter-Borchardt a question about just your -- one of the last things you mentioned was the coordination between the distribution system operator and the transmission system operator and that's something we've been talking about as we see potentially more distributed resources, starting in California, but in other parts of the country as well getting into the wholesale -- aggregating and getting into the wholesale market and how do you coordinate what they're paid in the distribution market versus what they're paid in the wholesale market and also how do you coordinate

operationally between the control centers?

And I'm interested in any lessons that you've learned. I know Germany, for example, has had an extremely rapid growth of distribution-connected resources and anything we should take from that as we figure out how our distribution centers and transmission centers should talk to each other.

DR. DIETER-BORCHARD: Well, unfortunately, you refer to Germany. Yes, it's true there we have almost 900 distribution system operators, very small ones even and serving less than 100,000 customers. So I don't think that that's the model that you should follow, but until now I must say the distribution side was left out of our development of the energy system; but as I have said already, now bringing massive renewables into the distribution grid now we have to deal with that. We have to deal with that to also reformulate the roles of the distribution system operators. We have to give them access to the flexibility because they have the first go on all the energy that is coming into their grid. And then because again we do not -- as in Ontario, we do not also want to now go for a copper plate. We also want now then to have the cooperation between DSOs and TSOs so to bring then this energy up to the transmission grid.

And what we are proposing now, so I cannot give

you the results, but what we are proposing now is, first of all, at the European level we have already a very strong European organizations, not lobby organizations, institutions representing the TSOs in gas and electricity and we have no such structure for the DSOs and that's what we are proposing now. We are proposing to establish not exactly in the same way, but similar to the GSOs, a DSO body at EU level. That's the first step.

And the second step then is, as I said, we are also tasking the platform that both organizations then have to build. We are tasking them with the different tasks where we then not dictate how they should implement then the cooperation, but we say on which fields they have to cooperate. For instance, data management they have to do, then the integration of the renewables, the planning and managing.

Cybersecurity these kinds of issues they have to work out codes and guidelines where necessary, demand side management the same thing. So all this they have to work out then in future from this platform and then it goes through the normal process. So it is a structural approach and task approach, but selected tasks.

CHAIRMAN LA FLEUR: Thank you.

I wanted to turn to our colleagues in North America here. Of course, Mr. Hewson, Canada's been a part

of NERC since its creation and we run an integrated grid. And Commissioner Madrigal, I know you recently signed a Memorandum of Understanding with NERC and have become more and more integrated with the NERC work. And by the way, I'm just struck by the fact that you're doing in Mexico things that it took 20 years here from opening the grid to setting up the market to introducing competition in transmission and everything in such a short time. It's just quite impressive.

I'd like to turn back to the conversation we had in the session before and ask Mr. Hewson and Commission Madrigal what you're looking for from NERC as you go through this transformation? We're all going through an energy transformation, but how this NERC and energy reliability enterprise can help and anything you want to contribute on that topic because we see you as partners in this topic we're working on today.

COMMISSIONER MADRIGAL: Yes, thank you.

I think for us cooperation is very important. We learn a lot. Our energy systems are more and more integrated. Of course, they are more integrated in the gas and liquid fuel sector, but what integrated in gas -- basically, what integrated in electricity is 40 percent of our production is from gas, so without recognizing that even at the ministerial letter Mexico signed with the DOE this

general principle for promotion the reliability, then we with the system operator and NERC sign them and will -- understanding we were already receiving lots of very valuable feedback from NERC. You know practices on reliability, sitting a standard, how to supervise, and basically the objective of this memorandum is to exchange experiences on physical infrastructure protections, cybersecurity operation and planning. So it was just basically for us a new step in the relationship because it has been so useful.

One of the areas that I see of importance going forward is with the opening of the power market in Mexico we see a lot of more interesting trading across borders. We have a historical interconnection with California and their collaboration has proven there it's always beneficial to both parties if we have common rules, common reliability standards. There in California we use many of the WEC standards. So going forward, I just see our two markets deepening a lot. We have many hearings at the Commission with in depth opinion from the U.S., from the different states trying to build transmission infrastructure to trade energy to Mexico.

So we need to, I would say, work a little bit more closely on cross-border capacity location, transmission rights, and of course, reliability standards as integration

gradually grows in other states. So I think it's just a natural progression similar to what you have seen in Mexico. But I just wanted to stress that the relationship has been very, very useful so far here.

CHAIRMAN LA FLEUR: Thank you. Mr. Hewson?

MR. HEWSON: Thank you. So I would second Commissioner Madrigal's point about inter-ties. I know that as we look the planning that the IESO is doing for Ontario the inter-ties play an incredibly important role both ways. You know we're an importer and exporter every year. And as we look at developing the renewable -- greater renewable energy in the system that becomes even more important for both sides, for New York, Michigan as they're developing their climate goals and they're implementing their new polices we want to be able to make sure that we work well together.

So I hope and understand from my colleagues at the IESO that NERC is taking those things into consideration and is considering the need for good flexibility across the systems to be able to integrate the changes in the way the supply situation is working. I think going forward the DSO side of things is going to become more critical for -- I know our ISO is much more closely working with them. I think that will slowly work its way up and there's going to be more coordination across those systems.

And I guess I would say, as an economic regulator, we're always looking for the standard-setting body to be taking into consideration that care about the costs of compliance, the cost of implementing new standards, recognizing that as the supply changes there are new cost pressures in the system, either from the renewables themselves or the different systems that have to go into place like storage to be able to make sure that you can manage that. And so we're constantly, as the regulator, looking to make sure the system is as efficient as possible.

CHAIRMAN LA FLEUR: Thank you. I want to turn it back to Michael, who actually has some recent experience in the European Union on an assignment, so I'm sure you'll get some staff questions.

MR. BARDEE: On my assignment, I was actually reporting to Klaus Dieter, so now it's payback time. And I actually do have a question for you, sir.

As you may know, in our country one of the issues we are facing now here at FERC is how to balance preferences of states to manage their resource portfolios to make their preferences known on generation and other resources, how to balance that with having regional markets and not having those markets distorted by the inputs by individual states.

You described briefly your proposal on capacity

mechanisms, which are, in sense, are tools used by member states have to integrate in some way with the regional cross-border markets that you're hoping to encourage. Can you talk about how that proposal is fairing so far?

DR. DIETER-BORCHARDT: Yes, thank you very much.

This does not necessarily mean if you have the energy mix left to the member states and you create a regional market that this is distorted. It becomes distorted when the member states put money into the development of one or the other technology and that is the point because you can have different energy mix in a region. Here a region means different members states together in a region and each member state has a different energy mix. This can perfectly work and we have the rule to make it work, but the biggest enemy is the state intervention in the national context, which then, of course, has a direct impact on the regional market and that's we have revisited the support schemes for renewable. I tell here example Germany. By the way, Ms. LaFleur, that's maybe a lesson learned not to repeat, what the Germans did. They were successful to boost renewables, but at the price that no other country can afford, so -- tariffs 20 years at a very high level is not the way to go.

We have changed the system. There is no feed in tariff any more allowed, so renewable support scheme have to

be market-based. They have to be auctioned and the price has to be tested through the market. So this is on the support scheme.

You mentioned the capacity mechanisms. It is a subsidy scheme, not doubt about it. That's the reason why we have said first the necessity has to be established at the regional level, not at the national level. Let's assume that you have in the Country A you have an adequacy problem, but next to it in the Country B you have a mothballed gas-fired power plant. It is not invented Belgium/Holland. Belgium has an adequacy problem because they have problems with their nuclear plants.

Next, 16 kilometers from the Belgium grid, there is a mothballed Dutch gas-fired power plant, so use it, make the connection, and use it. Here we had struggled with the Belgium government because they said, no, we don't trust the Dutch, so we want to have our strategic reserve. So all this comes in, but here, of course, that's the role of the Commission then to go into that and saying, look, this is the kind of state intervention that we cannot accept because let the market work. Because if you have the connections and you use all the potential of the regional market, then you get very, very good results, cost-efficient results, so adequacy assessment for the capacity mechanism regional level.

The other issue is there cross-border participation. So if they are allowed to design a capacity mechanism, it cannot stay national so others can offer because they have to tender. These are the elements that we are, from the European level, bringing into avoid the risks that you rightly pointed to, that if you have this -- every country has its champion and is going for it and supporting it that would have a devastating effect on regional market. So therefore we have a very strong state supervision by my colleagues from DG competition. You all have certainly heard about of them, so that's one of the tools.

And the other we are doing through the energy policy that we are trying to Europeanize support schemes whenever they are necessary and we are going for regional assessments instead of national assessments.

MR. BARDEE: One other question on a different topic then for any of the panelists. One of the issues that we have done some work on and may have more to do is as renewables continue to grow on our system we've tried to ensure that they are contributing the services that other generators provide, whether it's a primary frequency response or voltage or other services so that at an appropriate time and in appropriate way they are asked to bear their share of the burden just like other generators, and I wonder how you all are doing with that issue.

MR. HEWSON: Certainly, at the transmission level the IESO has been working with the large transmission connected wind facilities to look at increasing their ability to provide some of those services. At the distribution level, I think that's the next area that we're going to get into. Right now they've connected. The distributors have really taken on the role of upgrading their systems to be able to make sure that they can manage the effect of the renewable energy on the system. So I think it's an area that we're going to get into more, certainly being talked a lot about in Ontario, the need to make sure that all generators are providing the same types of services.

COMMISSOINER MADRIGAL: On the technical side, what we did as part of the first sort of independently set grid code, we review what has been Germany and Spain and the U.S. and there are very specific technical requirements on low voltage, ride-through capability, frequency response. So from the beginning we already included some of those more than requirements for large scale facilities because the experience of the past 10 years was that, yes, we need to improve. You know we had some all-induction machines, so we're moving to new technologies.

On the technical requirements also of the distributive level, we have a back-and-forth with the

utility with regard to inverters, so the issue of smart inverters. So we had a long discussion what is a smart inverter. Are you going to be able to use it where we ask the solution utilities, so the utilization part of smart inverters and the abilities you have to send signal I think it cannot be overlooked because we say we put all these requirements are you going to be able to use them or not. So we reached to a compromise in which we set some smart inverter light requirements for distributed generation resources in terms of the frequencies they have to stay connected or disconnected from the system, but I think the distribution level is going to be a learning process because not all distribution utilities are at the same level of maturity to use those technologies. Some utilities we saw in Mexico were struggling on how to understand then metering, the rule. How do I calculate the bill? How do I send the calculation, basic stuff? So when you move to the -- of the controls, it becomes a little bit more complex. So I really think, as our colleague from Germany, we need to work more on making sure distribution utilities work together to understand this new world in a more organized way because I think that's definitely a challenge.

On the commercial side, and although we're really moving really fast with the reform, on the pricing on ancillary services, they celebrated the work we were doing

on pricing, especially frequency response and reactive power because we have seen a tremendous interest of consumers to install storage, even medium scale. And you know for storage to say I want you to recognize the value I'm providing to the system. So we're thinking more realistically on how we should price ancillary services, so that any device if it is a storage or if it is a wind or solar plant is priced accordingly, so we haven't finished that yet. So we are working and I just thinking on how to do it so that the value provide by storage or wind or solar is recognized regardless of what technology is providing the service. So there we still have a pending task and we're trying to just learn as much as we can.

DR. DIETER-BROCHARDT: We as well. We are going first and foremost to the DSOs for the reasons that I have mentioned. Most renewables go into the distribution grid. That's why they need to have the access that they currently do not have to the extent necessary. But next to it, we want also to develop a market for our ancillary services so that we do not see that DSOs should have an exclusive right in providing these services.

Certain, yes, those are anyway covered by our network codes, but other services can also be provided through the market and therefore we are also very keen to develop certain ancillary services over the market and then

the rest producers, of course, they have to pay for it because they remain responsible if they cannot. And they cannot carry out this task themselves. They have to purchase the services over the market or if they get it from the DSOs, then of course it is included in the fees.

MR. BARDEE: Okay, so let me thank our three panelists and we really do appreciate your being here today, coming farther than anyone else on our agenda today. We thank you. And we'll come back at hour from now, 1:35.

(LUNCH BREAK)

MR. BARDEE: Thank you everyone. We are back for Panel Number Three headed as the Potential for Long-Term and Large-Scaled Disruptions to the Bulk-Power System. So I will start us off with our panelists, starting with Mark Lauby from NERC. Mark, please take it.

STATEMENT OF MARK LAUBY

MR. LAUBY: Thank you and good afternoon. I wish to thank the FERC Chair and of course Commissioner Honorable and the staff for holding the Reliability Conference.

At no point in modern history has the electricity sector experience a period of such revolutionary change. As to the theme of this panel, avoiding long-term and large-scale Bulk Power System disruptions is at the

heart of what NERC's mission is. In fact, NERC and the regional entities work with industry every day to identify risks to reliability, prioritize actions, and implement mitigations.

NERC uses a number of mechanisms for risk identification and mitigation. For example, the Reliability Issues Steering Committee identifies, prioritizes, and recommends mitigation of high and medium priority emerging risks. Some of the indentified risks include the changing resource mix, loss of situation awareness, extreme natural events, and cyber and physical security vulnerabilities. I'd like to focus on two issues related to the changing resource mix, distributive resources and single points of disruptions.

As Gerry mentioned earlier, the ERO Enterprise continues to scan the system for information that its collects for looking for faint signals, finding and addressing small risks today so that they don't become a bigger one tomorrow and this is, of course, evidenced by our recent technical report in the alert and affordable -- generation.

NERC will continue to scan for affects on the Bulk Power System, including monitoring the proliferation of distributive energy resources. We will focus especially on the changes in system characteristics and ensuring that

there are sufficient amounts of essential reliability services.

Secondly, suspending the supply of natural gas in the Aliso Canyon storage facility is a good study case on the vulnerabilities at the intersection between electric and natural gas industries. As an in depth review of this risk, NERC is completing a study on single points of disruptions, recommending, first, FERC run gas transportation as a reliable supply mechanism; secondly, periodic verification of dual fuel capability and availability. I understand it's getting harder and harder to build dual fuel plants; ability to obtain air permits or waivers to them anyway and increase planning activities, contingency analysis, and operational coordination between the two sectors.

I'm going to transition a little bit to resiliency. System resiliency is becoming an enhanced yardstick for reliability and I will cover resiliency in the context of two additional risks, one being extreme natural events and the second the loss of situational awareness. FERC, NERC, and regional entities are actively working together jointly on resiliency. In 2016, FERC and the ERO Enterprise jointly issued a report reviewing the sampling of industry restoration recovery plans. The report concluded that the plans were thorough and highly detailed and included 15 recommendations.

As a follow on to that study, a recent study was completed looking at the loss key situation awareness capabilities and how they may impact system restoration. Restoration activities that maybe difficult without these capabilities were identified, along with provided recommended methods, practices, and training.

Another example is the mitigation from the affects of space weather. In response to the Commission's directives, NERC developed two standards to address risks from geomagnetic disturbances. The first standard requires entities to have operating procedures that mitigate potential grid risks from geomagnetic disturbances. The second standard requires system planners to address risks from geomagnetic disturbances in system design and operation.

Further, NERC recently submitted to FERC a preliminary research work plan requiring an extensive multi-year effort using scientific and technical expertise from a variety of disciplines.

So in conclusion, and I know that's what you've been waiting, NERC's leadership role is essential to maintaining a focus on conventional risks, while anticipating emerging risks during a period of revolutionary change to the electricity sector. By putting a spotlight on key risks and their mitigation, working with industry and

with all our stakeholders, the ERO Enterprise endeavors to ensure a highly reliable and secure Bulk Power System.

So thank you for the opportunity to address these important topics and I look forward to discussions.

MR. BARDEE: Thank you, Mark. Next, we have Dede Subakti from the California ISO.

STATEMENT OF MR. DEDE SUBAKTI

MR. SUBAKTI: Thank you. First of all, my name is Dede Subakti. I'm with the California ISO. Thank you. Very honored to be invited to the nerd and geek party and I'm very proud to be a geek myself. And of course, it's really hot here today, but it is much nicer than being in California, where it's actually 110 degrees.

So today, I really only have two remarks really and the first one being the gas/electric coordination and we've been talking about Aliso Canyon since, what, it feels like forever now and the need to recognize how gas and electric coordinations and the need how to recognize gas constraint in the electric system itself. And the second portion is about the emerging issue relating to the inverter-based resources, the one that we've just been talking about with regard to the Blue Cut fire.

Really, each of these topics underscore the importance of a balanced portfolio, a balance resource mix that can provide essentially reliable services to support

operation of the Bulk Power System. So let me go to the first topic with the limited operations with Aliso Canyon. It's a concern for both gas customer as well as electric customers simply because that gas curtailment through generators could or may result in electric customer interruption.

So in the past few months, I myself, learned how important it is to have a robust coordinations between regulatory authorities within the state agencies as well as with the operating entities, so I made good friends with my peer at the SoCal Gas and working closely together as we're developing a lot of operating procedures with regard to outage coordination, for example, between the gas outage and transmission outage and generation outage. Day-ahead planning, that's another one and real time operations.

We actually learned quite a bit about how each other do our business. That's very interesting and very crucial. Really, life is never the same again in California with the limit operations in Aliso Canyon.

Now last year the Commission actually authorized California ISO to implement various mitigation to address this very issue. One of the mitigation measure that worked quite a bit is the utilization of new constraint in the California ISO market. What it is, is that a constraint that is put into the market optimization to reflect gas

limitation in the way that we dispatch our generations. It works really well. We used it in the past winter when it was really cold and it works in coordination with SoCal Gas System.

The authority to use this constraint is actually expiring at the end of November 2017, so currently California ISO going through stakeholder process to explore the extension of this authority in a more permanent basis and we also exploring the need and benefit to expand the use of this constraint beyond just Southern California, such as maybe in the western energy and balance market, the EI market.

So really based these lessons, we really request or encourage Commission staff to support and continue the efforts to look at the transmission service provider, transmission operator, market operator to implement adequate tools to mitigate gas system constraint in order to be able to operate the electric system reliably. We also believe that we should continue to foster coordination between electric and natural gas transmission operations. It's very important. We learned that we rely on each other quite a bit.

So while we have made significant improvement in gas and electric coordination, Aliso Canyon underscored a need for a balanced portfolio of resources and

infrastructures to help ensure BAs, such as California ISO, so we do not overly rely on one fuel source to meet our system need and can adjust to changing operating conditions.

While that's good, we have solar-inverter, solar. We have over 10,000 megawatt of transmission credits of capacity. In the past few months, we learned that we have a 1200 megawatt and that's just one event of many. So we have joint taskforce and in the report look for two risks in there. And based on these lessons learned, we believe it's important to have a standard, a reliability standard or clarifications of the reliability standards for the ability to ride-through voltage and frequency disturbance.

So at this time, I would like to conclude my remarks and thank everybody for allowing me to share these remarks and I'll be open and happy to answer any questions.

MR. BARDEE: Thank you DeDe. Next, we have Dr. Michael Kelly Rivera from Los Alamos National Lab.

STATEMENT OF DR. MICHAEL KELLY RIVERA

DR. RIVERA: Thank you. So David Ortiz and John Ostrich of DOEE and Eric Rolickson (ph) at DHSOCHI jointly initiated a research project at Los Alamos National Laboratory. The project's intent is to understand and model the impacts of an electromagnetic pulse generated by the detonation of stockpile nuclear devices on the transmission

and generation aspects of the U.S. Bulk Power System. The ultimate goal of this research to build the knowledge and understanding of nuclear MPs and their interaction with the BES that is necessary to develop a scientific workflow similar to TPL007-1, whereby the resilience of the USPES, the nuclear EMP can be evaluated.

At the outset, constraints were established for this scientific workflow. We would only consider a nuclear MP insult an event of concern if it causes two affects. The first is long-term damage to the BES requiring in excess of three days to repair and the second is that an impact of a significant portion of the BES resulting in an excess of $4 billion a day in loss economic activity to the United States.

We've completed the first two phases of this work and these phases, nuclear EMP insults were parameterized. You can see the parameterization on the second slide of the set of slides you have in front of you and a list of benchmark events also on Slide 2 covering this parameterization we've generated. And we've begun to determine which of the benchmark insults were most likely to rise to the threshold of the study constraints.

I'm going to jump straight to discussing the five benchmarks XO atmospheric nuclear EMP insults that are enumerated in the handout. I want to stress these benchmark

events do not correspond to any particular nuclear weapon or weapon delivery capacity. If the did, I would be leaving in an orange jumpsuit. Rather they have been chosen to clearly delineate regions of interest where certain EMP effects, for example, the E3 heave or the E3 blast or the E1 phase of the first are dominate.

I'm not going to go into the extreme detail on each of these benchmark events. Their expected impact to the BES is shown in the table on page 2 based on our current and previous studies. I want to note that there is a slight error in the table. The impact from the 25 kiloton 100 kilometer case should read a medium with a 200 kilometer case reading high. We'll get to that if you ask questions later.

I'm going to stress two important points about E1 that we are finding in our analysis and back those points up with data that is presented later on in the later pages of the handout. The first point that I'm going to stress is not a new observation, but it certainly is an observation that is not advertised well enough. Those of us familiar with EMP know about smile diagrams very well. A smile diagram is a general form for the radiated hazard field present in the E1 part of the electric magnetic pulse created high altitude EMP insult.

The E1 smile diagram for our five benchmark

cases is shown on the third page of the handout. Naively, one might assume that where the electromagnetic pulse is strongest the largest currents will be generated on cables and lines. This line of thinking leads to worst-case values of coupling, the worst-case current peaks, as shown on the next figure or the next page.

If we look at the table to the upper right reporting magnitude, for a few of these benchmark events the pulses can exceed a megavolt in size if we think about the coupling this way. This coupling, however, is completely wrong. The efficacy with which the E1 component of EMP can couple cables and lines is determined by more than just magnitude. It's determined by the phase angle of the electric field as well as a bunch of other things.

When these constraints are incorporated, the realistic coupling hazard is shown on Figure 5. I'm not going to go into extreme detail, but the important point to take from this is that the magnitudes of the fields are now down by a factor of 3 in some cases and even more. So the important point to draw from this is the necessity to have a complete workflow that incorporates all of the elements from one phase to another. You cannot just simply hand off the magnitude and expect the engineers to do coupling without any sort of context and without any sort of other constraints.

And the second point I want to make is about the konus covering EMP event. For our benchmark events, this corresponds to the 400 kilometer burst altitudes. The peak radiated hazard fields and conducted hazard fields drop off precipitously at these altitudes. For the 25 kiloton case, in fact, the radiated hazardous fields dropped by almost a factor of 5.

We are not ready at this point to conclude that this means that the konus covering events are of absolutely no concern, but we can say that the lower altitude burst events, though affecting a smaller area, have a significantly higher chance of damaging BES equipment within the area that they affect. Thank you.

MR. BARDEE: Thank you, Dr. Rivera. Next, Dr. George Baker.

STATEMENT OF DR. GEORGE BAKER

DR. BAKER: I want to thank Chairman LaFleur and the other FERC Commissioners for the opportunity to speak today. I'm a senior advisor to the Congressional EMP Commission. I'm filling in today for Mr. Earl Gjelde who is the former COO of Bountiful Electric Power Administration and Undersecretary of the Interior and he regrets his inability to attend.

I want to discuss EMP together with cyber and physical threats, the EMP Commission, the charter we're

looking at all three affects, the combined affects and what I want to do in the time I have is discuss a vision for the future where the power systems will be able to operate through, will recover quickly from these what we call triple three contingencies. And there's a huge possibility of common ground here. If you look at what the industry is striving achieve and what the EMP Commission there's a huge overlap and just stress that.

So the first point of the vision is that the industry and government would be working together to achieve the resiliency to these combined affects and private public partnerships are essential and there's already some very good examples of these in force. The infragard, the EMP special interest group and several public/private national exercise -- Army War College, National Defense, University NARUC and U.S. National Guard Association is examples.

Also, another good example of late is Duke Energy is working with state and local infrastructure service providers and emergency responders at Lake Wiley to develop a plan for EMP protection.

Now the U.S. Military has proven EMP protection approaches that can be translated directly to a large part of the grid infrastructure. And I'm concerned and disappointed because there's been inadequate sharing of the DoD insights with the power industry and DOE and EPRI and as

a result there's a lot of work that's being done that's really reinventing things that were already known and that's a problem. That's going to complicate the playing field.

The second point in the vision is the electric utilities is able to recapture the cost for protection. And here I'm not going to go into any detail because Tom Popik will cover this.

Third, we need better models, national-level models of grid affects and recovery steps and I think Los Alamos is already onto this, but in order to have priority system hardening, safe shutdown, and expedient reconstitution we need better models and model development will be greatly aided if industry historical databases are made available to us. We have also yet to perform test to failure validation for large transformers and generator stations. That'll be every important to know where these things actually failed.

Fourth, a vision point is a coordinated national level Black Start Plan and resources that are exercised on a regular basis. We have Black Start plans mandated for limited blackout contingencies, but there's presently no national plan addressing restoring the grid following a large, long-term outage. A big difference between a normal Black Start, if you want to call it, and a long-term outage Black Start is the absence of functioning neighboring

regions. So when you get into local preparedness, it becomes all the more important there.

Also, the communication assets used under normal conditions will likely not be available due to EMP and GMD affects, such as land mobile radios and UHF SATCOM maybe the only communications available and these constraints need to be included in planning and exercises.

And finally, we need -- and this is a point that Commissioner Gelde (ph) wanted me to stress that the FERC/NERC Consortium is not set up administratively or legally for national security problem resolution. And we believe on the Commission that a national electric power protection executive is needed, reporting to the National Security Council and that executive should be vetted with the authority to establish protection and assessments guidelines.

So those are the points. That's the vision. And I hope that this will help focus our efforts to protect the grid. Thank you.

MR. BARDEE: Thank you, Dr. Baker. Next, we have Dr. Randy Horton from EPRI.

STATEMENT OF DR. RANDY HORTON

DR. HORTON: Thank you, Chairman LaFleur, Commissioner Honorable, FERC staff, and fellow panelists, EPRI appreciates the opportunity to participate in today's

technical conference. So my comments here today are going to address the question that was posed to the panel regarding manmade electromagnetic pulse. I will provide a brief overview of the work that we're doing as well as some of the knowledge gaps we're attempting to address with our research.

So April 2016, EPRI initiated a three-year research project to address the potential threat of how altitude to the resiliency and reliability of the Bulk Power System. And today I'm pleased to say that the project has financial support from nearly 60 U.S. electric utilities.

I will refer you to my written comments regarding the details of our research plan, but the primary objectives of the plan are, one, improve understanding of the potential impacts of altitude to EMP and we're looking specifically at E1, E2, and E3 on the Bulk Power System through extensive laboratory testing and computer-based modeling; secondly, develop software tools, techniques, and guidance that could be used by utilities and others to help assess the potential impacts of HEMP on individual assets and the Bulk Power System as a whole; three, to develop cost-effective options to help mitigate the potential impacts, and fourth, to provide timely communication of our research findings to our supporting members and stakeholders, as appropriate.

Through our collaborative research model, EPRI is bringing together experts in electric power systems as well as those versed in the phenomenology and effects of -- EMP to improve threat assessments to the Bulk Power System. For example, we're working closely with the Department of Energy, Lawrence Moore National Lab, Sandia National Lab, and Los Alamos National Lab, which I can say Mike and I've become close friends over the last year or so. And we're also in communication with other agencies, such as FERC, DHS, and the Defense Threat Reduction Agency or DTRA.

I will now quickly transition to our E3 assessment that was published in February of this year. Due to concerns expressed over the potential loss of a large number of bulk-power transformers which could lead to a long-term blackout, an initial focus of our research was to determine the potential impact of E3 on these assets. The EPRI Study evaluated the potential impacts of E3 from a single altitude nuclear detonation over 11 different national target locations in the continental U.S.

Details of the study are provided in my written comments, but in short, the results of our study indicate that although a significant number of bulk-power transformers could experience GIC levels above 75 amps per phase or more, and that's the screening criteria that's in CPL7. Only a small fraction, 3 to 14, depending on target

location evaluated would be of potential risk of thermal damage.

These results can be used to help quantify the overall risks of E3 impacts on the Bulk Power System, but I want to stress that they should not be interpreted to indicate that E3 will not affect Bulk Power System reliability. The potential for widespread outages due to voltage collapse and the combined affects of E1, E2, and E3 together are still being evaluated. Although, the E3 research is continuing, a significance focus of EPRI's research efforts in 2017 and beyond are related to assessing the threat posed by E1 and E2 and developing the capability to evaluate the combined affects of E1, E2, and E3 simultaneously. We believe that the latter capabilities is vitally important in understanding the true impacts of HEMP on the Bulk Power System.

In conclusion, the potential impacts of HEMP are real; however, there are many open research questions that need to be answered before risk-informed decisions related to hardening and mitigation can be made. EPRI is committed to developing science-based solutions to these difficult problems and will continue to offer technical leadership and support to the electricity sector, public policymakers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity.

Thank you again for the opportunity to be here today. This concludes my testimony. I look forward to any questions you have.

MR. BARDEE: Thank you, Randy. Next is Tom Popik from the Foundation for a Resilient Society.

STATEMENT OF MR. THOMAS POPIK

MR. POPIK: Thank you Michael Bardee. And at this point, the usual thing is for the panelists to thank the Commission for the opportunity to testify. In this case I would like to doubly say that. The Foundation for a Resilient Society is usually a dissenting voice, but for the second year in a row we've been invited to testify here. And I would just say that open debate is alive and well at FERC.

I can sit next to Dr. Horton here and we can have a debate in public and that really reflects very well, both on FERC and our country. And so I'll just briefly say something about Dr. Horton's testimony. In terms of the 3 to 14 transformers that would be impacted, we really have a small base of real world tests for that conclusion. Is it correct there's only two actual hardware tests for transformers that that was based on?

DR. HORTON: I believe that's correct.

MR. POPKIN: Okay. So we're a great nation. We have hundreds of millions of people to protect and we really

should be able to devote the societal resources to having tested more than two transformers and not even to failure and not at full load; is that correct?

DR. HORTON: Not to failure.

MR. POPKIN: Okay. To come to these kinds of conclusions that are so important to our society. So I'll get into some of the substance to my testimony. The staff, one of the prompts for this testimony is the question of long-term outage and it's really a very important question. We have about 10 pages of testimony. I can't go through it in the next two and a half minutes, but I would refer people to the testimony, which I believe has been put online by the Commission at this point and I also have paper copies with me.

But briefly, if we were to a long-term outage, everybody in this room could potentially be in danger. What is a long-term outage? It's an outage that persists longer than the resources of backup power for the Bulk Power System and supporting infrastructures and over an area so large that significant outside assistance would be impractical. We have a scenario for actually the eastern part of the United States in my testimony today and I would really encourage people to go through that.

I have some more remarks also about what really drives reliability here in the United States and the

constraints that we, as a society, are put under. And I would start off by saying that so much of Mr. Lauby's testimony today and Gerry Cauley's testimony earlier, the Foundation for a Resilient Society really agrees with. When they start talking about gas/electric interdependence, the need for fuel diversity, and the need for spending generation for frequency support and for reactive power, especially in places like California, a lot of these technical reports that are coming out of NERC are really excellent and we do hope that the Commission pays close attention to those reports.

And also in my testimony today, we have a lot of quantitative analysis which supports those findings of NERC. And I would also say, very briefly, one of the fundamental problems is that the market, especially the organized markets, do not appropriately value reliability. And we have, again, good quantitative analysis for this in my testimony today.

And finally, on the last page of the testimony of Resilient Society, we have some very specific recommendations for the Commission and the Commissioners and we hope that they examine those closely. And I'd be happy to take any questions about those recommendations. Thank you very much.

MR. BARDEE: Thank you, Mr. Popik. And finally,

we have Sylvain Clermont on behalf of the Canadian Electricity Association.

STATEMENT OF SYLVAIN CLERMONT

MR. CLERMONT: Thank you, Mike. Bonjour Madame President (speaking French).

Commissioner Honorable and Mr. Bardee and FERC staff thank you for the opportunity to participate in this discussion about reliability and to take the time so we can have a discussion on the reliability. And it is also an honor for me to represent my fellow Canadian colleagues.

It's been said, but it's probably useless to remind anyone about the integrated nature of the electric grid, but let me do it anyway because we must be looking at solutions together. We are in this together. Today's threats, including the one we'll be discussing in this conference are cyber/physical security, extreme weather events, CMP, GMD, you will all agree are all very different. They're varied in nature. They're complex and most of them are evolving. So preparing for one does not necessarily prepare the grid for the other one. But still, we must prepare for all of these and the threats don't know yet, so solutions probably must be on the same nature. They must be varied. They must adapt and we suggest we must take an all deserved approach to resiliency instead of focusing on each of these threats individually.

So what do we do? Well, certainly, careful analysis to learn and understand the threats and their impact and the network behavior resulting from these threats is important. Risk identification like NERC is doing that is proactive action, looking forward trying to anticipate where your bigger risk will come and trying to understand what will affect your network in the year to come.

And at entities, each of us we should continue to study our studies to better understand the impact on our own network. That should result I call them intelligent investing at strategic and critical points of our network. So out of these analyses we understand where are the weak points, if I may say, of our network, so intelligent investing to make those weak points or strategic points more resilient.

Managing carefully inventory spare parts. We've been talking about spare part transformer for a while, but a bunch of spare parts for your critical equipment, so I call that managing carefully inventory and of course collaborate together, including collaborating with regulator and have open discussion with regulator. Sharing information between industry, government, and regulator, we keep saying that, but that is really key to making good progress, using the forums even more. The forums like the NATF and the GATF offers great spaces for candid discussions.

Continue and expand the exercise like the grid-x. Grid-x are a great learning experience for all of us -- government, industry -- so we should continue those and expand those.

In Canada and with the U.S., we did recently the U.S./Canada electric grid security and resiliency strategy. That's a start. We should continue to work on that and work on the actions that are in that document. We also must keep in mind that as regulator and our customers want us to spend wisely the money they give us we must be careful about where we spend to make sure that we spend on what matters most for reliability.

All of these threats, of course, including the I- impact can't be ignored, but I believe they must be addressed with broad solutions that make the grid more robust and more resilient to anything.

And finally, standards -- and maybe we will be discussing that more -- standards are not the only tool in our toolbox and may not be actually the most efficient tool in our toolbox. We have alerts, guidelines, best practices, lessons learned. Are there ways to improve on those? Are there ways to follow ups on best practices? So like alerts when they are issued, you must respond and say, okay, I did what's in the alert. Could we expand for best practices? It's an open question, but these are tools in our toolbox

and they probably can be used more.

And lastly, remember no on entity, no one agency can work in isolation to find a solution. So that concludes my testimony. Many thanks for your attention and for the opportunity and will be pleased to discuss any question you may have.

MR. BARDEE: Thank you Sylvain. We'll start our questioning with Acting Chairman LaFleur.

CHAIRMAN LA FLEUR: Thank you. Well, thank you all very much and merci beaucoup, Mr. Clermont.

Okay, I'm going to start with Dr. Horton. As you probably know, I was recently hauled up to the Hill to testify about EMP and it actually was a great experience because as always when you testify it meant I spent several days really preparing. And I testified that the Commission has been quite deliberate in not directing an EMP standard thus far as we have directed physical security, GMD, and other things because we didn't believe that we had a clear enough path to where the best place would be to require thousands of transmission owners to spend their money to protect the grid against the biggest risks. And I got into a little bit of a sparring with some of the other folks on the panel about whether the physical securities studies or whatever how we would best get at that.

And I pointed quite repeatedly to the Los

Alamos, Idaho, and EPRI work as potentially yielding that information about how we best actually protect the grid. And I see in your testimony, Dr. Horton, and I invite others to chime in too, that some of these pieces of work from EPRI are coming quite soon, third quarter this year, fourth quarter this year. Do you think those pieces of work will give us actionable information that we can use decide what to do about the grid or are they a step on a path? I mean where are we in really understanding this.

I would love to be able to do something about while I'm here, and that's not forever, so where are we?

DR. HORTON: Right. With my EPRI hat on, I have to be kind of silent on policy issues, so I'll speak strictly from a technical standpoint. So at a high level, if you're asking me from a technical standpoint does the knowledge, the tools, and guidance, and so on exists to do kind of a TPL8 type of standard I would say the answer is no.

So basically, our research project we're not really even getting into the risk piece. We're assuming that the blast happened. We're looking at really what are the true impacts and ultimately how would you develop cost-effective mitigation options to mitigate against those impacts. So we're doing this as quickly as possible, so you know this is a three-year research project, but it's not

three years of research and then the data dump. So actually, as we get to a point where we feel like we have some actionable information, we're providing that to our members. And I would also say to the public as well so as a part of public benefit mission we always evaluate our research deliverables to look and see, okay, EMP is a very important topic. Would this make sense to put these deliverables out in the public domain at zero cost? There're always in the public domain.

So for example, the report that Tom mentioned you know we did the assessment and we didn't just do the assessment and say here's the answer. We did the assessment and said here's what we did. Here's the input data we did. Here's the models we used. That's how you're able to know that two of the models were test. We're providing all that detail so that we can have these robust discussions like we're having today, but in short to answer your question, I think, ultimately, at the end of the project when we're able to do what Mike mentioned, which is this workflow, which is look at the impacts of E1, E2, and E3 together we'll have bits and pieces along the way, but we really need to get to the point where we can study all that together to really find tune what the potential hardening options might be.

DR. RIVERA: The workflow can't be understated

here. There's a lot of missing pieces to EMP, but there's also not kind of universally accepted workflow. Don't worry. There are workflows out there. IEC has a set of standards that you can follow. The quantitative workflow from end-to-end that's agreed upon is important here. I mean to go back to kind of the what happened with TPL007. TPL007 put the workflow out there and then people came in and beat up the workflow and different piece of the workflow are now being looked at and maybe we substitute a number here or we add this piece there.

The same thing needs to happen here. We need to have an accepted workflow so that way scientists can come and have a context with which to go, okay, this is wrong here. This is right here. We have to change this and allow this workflow to evolve to eventually something that could be actionable.

DR. HORTON: And quickly, one thing I wanted to add, you know it's easy enough to build a block diagram, which is the actual workflow, but the real missing piece is the actual tools, like they have to be built essentially from scratch or figure out some way to cobble together the different types of tools. That's another thing we're working on.

CHAIRMAN LA FLEUR: Well, thank you very much. I'm most concerned about E1. I certainly agree that our job

at FERC is not prevent it. Our job is oversee the construction and operation of the grid to mitigate various hazards and I think we have -- my understanding and I'm not an electrical engineer, as is probably obviously, but I believe we have our arms around E2 because it's like lightening and we've done a lot of work on E3 like things in the GMD context, but E1 is where we really need the work that gentlemen are doing, I think, to have an intelligent mitigation strategy.

DR. RIVERA: Just to jump in, E2, generally it is said that, yes, it's a lighting-like strike and we're hardened to lighting, so everything's okay, but this is an assertion and it's something that really does need to be investigated. I am not saying I disagree with the general sentiment, but it's something that has not even been remotely investigated.

CHAIRMAN LA FLEUR: Well, that makes your work even important. So bearing in mind that we're waiting quite eagerly for that work, I want to turn to the question I think Clermont keyed it up of how can we build resilience of the grid against various risks? I'm encouraged by some of the things have been done recently on transformer sharing, with grid assurance and so forth. I'm also slightly optimistic that those sharing programs will lead to more standardization or perhaps standardization. I mean I

believe strongly that if this industry knew what it wanted in terms of mitigation it could go to ABB and Siemens and so forth and they would build it because we have -- you, collectively, have a great deal of buying power. So I think we're making a little bit of progress there, although I'm happy to hear more things we could do. But I'd like to know how do we actually design redundancy and so forth into the grid.

Of course, I read Mr. Popik's testimony, but we can't turn back the clock and say we want -- we're going to live with the system that has a lot of renewables and a lot of demand resources and a reliance on natural gas. So how do we build the Bulk Electric System to be more resilient? Are there things we could be doing in terms of -- I'd hoped that the operating procedures part of GMD would help by kind of planning in advance, islanding. We have all these experts here and appreciate any ideas how we can build it in on the front end.

MR. CLERMONT: Well, if I may take a first shot. I think what we learned from our famous ice storm in the end of the nineties.

CHAIRMAN LA FLEUR: I remember very well. We weren't too far away.

MR. CLERMONT: Well, you were in New England at that time, yes, so probably a lot of your employees came to

help. And you remember that the --

CHAIRMAN LA FLEUR: As did yours come to help us many, many times in your gray trucks.

MR. CLERMONT: Thank you. But may remember that some part of the province were out of power for three months, so I think that qualifies as a long-term outage that we're talking about. Obviously, not large scale, but a fair amount where a good share of the population was living -- was out of power for three months. So what did we learn? So we took a careful look at our network and said, okay, why? And then we came with design criteria. We review and revised our design criteria, moving forward. So all new lines must sustain more ice, more wind, more of that and more of that, but that's 20 years ago. So all the new line we build in the past 20 years are stronger. They have anti-cascading towers. They're able to support more ice and we added stronger structures.

We looked at the grid and we saw that a lot of substation were already connected to another one, so we built a couple of lines to make sure that they looped so every substation is connected to more one of its friends. And we look into remedial -- what's called RAS now, Remedial Action Schemes, to see how that could help. And we're still today looking -- we performed last year another critical look at the network.

I was talking about weak points, but after 20 years of doing that where do we believe there's weak points? Where do we believe I call them intelligent investments could be made, so one more transformer there, one more line there, one more substation to make sure that there's more loops, that there's stronger structures. It's not magical, but I think it did the job.

If were to have an ice storm like the one we had or any actually extreme weather events our network would not sustain the same amount of damage. So that's not a miracle, but it's a careful, small investment, look at what was weak, and we can all do that; but we will need an open conversation with our regulators because it will require investment. And the investment when we increase load or capability of the network are usually easier to understand for everyone, but now we're talking about money to get the same service. These may be more difficult conversations with the regulators.

CHAIRMAN LA FLEUR: That's why I'm asking the question because I would like to be a champion of building more resilience and having been around this industry for several decades I find -- and I think this is just human nature. There's a tendency to respond where it happens to what happens, so Quebec is ready for ice storms, also you did a lot of work on (0:44:07.4) disturbances after that

happened.

New York City has built its substations to endure the next Sandy and bigger than Sandy. New Orleans is ready for another Katrina. They've built the best levies in the world. You go several hundred miles away and they haven't necessarily applied the same lessons. And so that's what this continental effort is about broadening those lessons.

MR. LAUBY: Just to add, to me it comes down to basic planning and risk identification and mitigation. And of course, we've been working hard on that at NERC and with industry and identifying what are some of the risks that are existing today with the faint signals that we hear and do something about them. And also looking forward as we see more and more variable generation coming online and it's going to be always synchronous of inverter-based. How are we going to get inertia out of that? How are we going to sustain frequency? How are we going to sustain voltage in that kind of world? Let's make sure we put a spotlight on those kinds of things so that we don't have to be looking in our rearview mirror saying I wish I would've known about that. So there's a lot of things that industry does to ensure that the system's reliable. They ever get a thumbs up saying -- nobody calls them at 3:00 o'clock in the morning and say, look, it worked great.

Yes, so that being said, I think we have to be vigilant. And if you read over Mr. Popik's materials, he's identifying some of these risks as they come on the system and so what do we need to be doing now to ensure that we're ahead of it so that we've been able to ensure a highly secure and reliable Bulk Power System?

DR. HORTON: I'll just make one quick comment and kind of zero in on a particular problem, but with regards to like safe transformer impacts due to GIC, either due to B3 or GMD event, I think there was a couple of things. Our recent E3 report and research basically if you look at the way we did the study transformers that were maintained properly like if you were in good condition we didn't see a lot of issues. So you know improving maintenance activities. And then secondly, a lot of utilities are beginning to include GIC specifications in their transformer designs. I think that's another kind of low-hanging fruit action time that could be employed.

CHAIRMAN LA FLEUR: Thank you. And just to pick up on something Mr. Lauby said, there's always enough money after it happens. I just want to ask one more question because I can't let you go without asking a GMD question.

COMMISSIONER HONORABLE: I was wondering.

CHAIRMAN LA FLEUR: Well, I've been closely following the -- well, first of all, thank you for the

research plan, which has quite a lot in it. And I've been closely following the budget of the U.S. Geological Service and I'm wondering -- I want to just hear how important the work that they do is to the operating protocol standard, the ongoing work plan because I had thought we were quite dependent on real-time satellite data to understand what's happening with space weather, but I have the experts here. Because it's just something I've been really watching. There's been a lot of debate about the USGS budget.

MR. LAUBY: I think that the work that they were doing, especially around mapping resistivity was extremely helpful and there are other ways, I guess, that we can get at measuring of that resistivity, but it allowed us to get a much more of a microscopic view of the resistivity and an understanding of what the ultimate -- occurrences are.

CHAIRMAN LA FLEUR: Anyone else?

DR. HORTON: I would just say that having the magnetometer data and also the Earth model data is critically important with anything to do with GMD. And even the E3 I mean the Earth model piece of that is very important.

DR. BAKER: I would echo that the Earth connectivity models are extremely important and one of the ways to get at that is to make more measurements and correlation between GIC and the magnetometer data. That

needs to happen.

MR. CLERMONT: That won't be very useful for you, but in Canada we get those data from Natural Resources Canada, so we're not depending on that.

CHAIRMAN LA FLEUR: It's useful as a good example. The kid next door does their homework on time. Okay, I'll turn it over to Collette.

MR. CLERMONT: Well then, maybe it is useful for you.

COMMISSIONER HONORABLE: Good afternoon, gentlemen. Bonjure, sir.

MR. CLEMONT: Bonjure.

COMMISSIONER HONORABLE: I'm delighted to engage with you all and I want to apologize for returning late. I was at a luncheon and the speaker was Dr. April Erickson from the NASA Goddard Space Center. Believe it or not, we were almost talking over each other talking about this very topic and how almost in vogue it is, not because it's the most popular topic, but it's because we need to be focused on it. And I want to thank each and every one of you for the ways in which you have blended you expertise.

I, too, am a lawyer by trade and so this -- I'm not an engineer, but what I do know is that scientists and engineers you work by testing and challenging and finding the proper dataset and making sure that the modeling, that

sensitivities and the futures are the proper ones so that as we get more robust data we will be able to put it into some modeling process and come out with something that we can use. So really this discussion here today has given me some comfort, Cheryl, about our course with the GMD effort. And I want to thank those of you who have participated with us along that journey.

And to our Canadian friends, thank you. When I arrived here at FERC, one of my first meetings was with you all and you reminded me about how our work impacts our friends to the north, so thank you for also engaging with us.

And to Mr. Popik, thank you because you've touched upon this open process we strive to have. That's why we have so many panelists because we know that there are a lot of views and we don't want everyone to come and agree. You all, even disagreeing at times, though in an agreeable fashion, help us carry out this work better. And you testing our thinking and the ways in which we are proceeding help us and educate us. So regardless of whether you're at the table, and I know you always do, you file those comments. Please continue to do that because it so helpful to us.

Mr. Lauby, I acknowledged to you, as you know, in the other panel with Gerry Cauley, but we're so grateful

to all of you for your work on this topic in particular because it's one that challenges me personally because we don't have years of data and occurrences, thanks goodness, that would really help better inform our work.

I want to ask a question, and it goes back to something that Cheryl touched on. And I want to first start with Dr. Horton and I want to ask any of you to chime in. And let me thank every -- in full disclosure, I served on the Advisory Committee for EPRI, but I learned a lot about the ways in which EPRI is supporting the work in the sector, looking ahead at what's coming around the corner. I was very appreciative of this particular study.

I have to tell, Dr. Horton -- I call him Randy.

DR. HORTON: You can call me Randy.

COMMISSIONER HONORABLE: Thank you, Randy.

There was quite a bit of discussion. One, I think people were excited to see it, but two, I think there was an interesting question about why start at E3? You know if you think about -- and I've had to educate myself. I have just enough knowledge to be dangerous here. If you're thinking about E1 scenarios, I agree with Cheryl. Those are the things that I tend to be concerned about, especially the early time pulse events.

E2, as Dr. Rivera said, could be maybe lighting, but he said we really need to learn more about that in order

to say for sure. And then what appears to be the most significant event, the E3, which may not happen as often, but boy, when it does it will certainly get everyone's attention. Tell me, and forgive me if you've talked about this, how did you arrive at starting with E3? And let me also say that I'm grateful that you will turn to look at E1 and E2 because I think altogether it will provide a wealth of information for us.

DR. HORTON: So we made the decision I can say, and you probably are aware of this based on what you just said about some of the discussions you've had. We had some very robust I'll say discussions about why we chose to go with E3, but really it was simple. We did realize that if you lost a large number of volt power transformers you would have a blackout that lasted for a long time and then that kind of changes the whole landscape. So right off the gate we wanted to see, okay, if we took some of the same studies that had been done in the past, but sort of update those with some of the newer modeling capability that we have, we wanted to see would we get the same answer.

Based on what we did, we didn't get the same answer and that was the reason we felt it was very important to put all of those details in a report so we can have a discussion about what we did. You know people may not agree with it, but we can talk about it and so on.

That said, in our study, we were not able to include the effects of E1 or E2, which you know if you think about how this might actually work in reality is you have the E1 come through. You may damage some electronics. It could affect relaying and how the system would respond when you'd get to the E3 piece, but we feel like our analysis was conservative from the E3 effects on transformers, but when you start to look at what the overall system impact is you really do need to include all there. So we're trying to get to a point where we can model those -- essentially, model those all together so that you really know what the full impact is. That's kind of a long answer for a short question.

COMMISSIONER HONORABLE: And I don't know if anyone else wants to chime in this topic in particular, but if not, I'm going to proceed.

Dr. Rivera, I want to thank you and your colleagues -- I mentioned to Dr. Rivera before we began this morning how grateful we are for the work of our colleagues at DOE and especially you and your colleagues in the national laboratories. We rely heavily upon your work and it's beautiful how we have come to rely upon that in our rulemakings and our decision-making and so there really is a role we all play in holding this grid and making sure it's reliable and resilient, so thank you.

I want to press on you a little bit more about the E-2 areas to the extent that you're willing to discuss this. What could we do to learn more about the sorts of events that are likely to occur in an E2 occurrence and if there are things that we should be working as regulators and policymakers in this area?

DR. RIVERA: The short answer there is I don't have a good answer for you. There's just not enough done on E2. We have E2 simulators to some degree. We have E3 simulators to get to ground fields. There is, so far as I know, no direct E2 simulator with which we could even get ground fields.

Now this is not to say that this is a difficult extension of what are currently codes that out there. It just has not been done, so I wouldn't even know where to begin on answering that, but it is some research that needs to happen to ensure that this assertion about E2 is not going to have an effect is adequately researched. So just out of an adequacy of concern, basically.

COMMISSIONER HONORABLE: Thank you. And I hope that some of your colleagues have heard that. In case they're twiddling their thumbs, they can get to work on that.

DR. RIVERA: They are well aware and they are working.

COMMISSIONER HONORABLE: Well, very good thank you. And I feel confident that if you aren't aware, then there is certainly a lack of information because you are a trusted source for us and I appreciate your candor there.

Mr. Popik, I wanted to turn to your recommendations. You teed it up and I wanted to bite. So in your pre-filed testimony, you have us lots of recommendations. Thank you for those. I'm interested in one in particular and it happened to be the last one because in it you spoke about FERC's need to advocate and engage more with Congress and the FCC regarding communications, in particular, in ensuring resilience. I take that to heart. I think a number of us, as regulators, were really aware of our lack of coordination after, for instance, Hurricane Sandy and inoperable we are in and how interdependent we are and we can't communicate about getting the lights on if the communications network isn't up and the folks in the communication sector can't do their work if they don't have energy. And so we know that there is a symbiotic relationship there.

I agree with you that we haven't done enough and especially after not only Hurricane Sandy, but any number of events that have occurred. And I wanted to ask you in particular specific recommendations you have since you've teed up the issue.

MR. POPIK: Well, thank you very much for that excellent question. Before I get into the heart of it, I would say that already FERC coordinates with another important agency, which is the Nuclear Regulatory Commission and you have that annual meeting. I think you recognize, as the Commission, the importance of that symbiotic relationship between nuclear power and electric reliability. The same is becoming ever-increasingly true for communications and the Bulk Power System.

NERC and Mr. Lauby, in his testimony, referred to this. I'll just briefly give you the history in terms of resilient communications at the FCC. With Hurricane Katrina, a lot of communications were out and it became very apparent how critical communications are. There was a post-Katrina panel that recommended great resiliency of communications and the FCC actually passed a formal rule for greater backup power durations among what are called central offices and remote terminals.

Unfortunately, there was some opposition to that and ultimately that greater resiliency for backup power was placed aside by the D.C. Circuit Court and that's really where it rests right now. I think that FERC, as a Commission, would have very significant authority if you were to go to the FCC and potentially establish the same kind of regular meeting framework that you have with the NRC

and so that's really the heart of this recommendation.

COMMISSIONER HONORABLE: Well, thank you for making it. And I recognize it's something we certainly should consider it and I'm saying this out loud because I'm sure that our future colleagues, whether or not I'm here, will take this to heart. And our engagement with the NRC is quite robust and we learn so much from one another. And even with regard to rulemaking and licensing and permitting there are just a number of ways in which we are aligned, including our work with regard to reliability and resilience.

I appreciate you harking back to Hurricane Katrina. I recall days being chairman in Arkansas at the Commission and dealing with coordinating and coordination after tornadoes and after a significant amount of infrastructure was taken down. I also when hearing you speak recalled testifying before Congress before a subcommittee about responding to severe weather events and the need for the energy sector and the telecom sector to better coordinate.

But in saying this I also would say that's why the state processes are so important too, that the first responders and emergency management and every one along the spectrum also needs to be engaged. And so I appreciate that you make the recommendation and I'll certainly keep it in

mind.

MR. POPIK: Thank you.

COMMISSIONER HONORABLE: And I believe I will yield so that the staff can ask questions. Thank you.

MR. BARDEE: Thank you, Commissioner. I have a couple of areas I want to touch on and then I'll turn to my colleagues here. One of them starts from the Aliso Canyon scenario, gas dependency as it increases in our country and more specifically, the planning that might be necessary or appropriate to foresee and prepare for similar circumstances elsewhere.

We have transmission planning standard now that, in some sense, has that element in it. It applies to transmission planners and planning coordinators and it says in certain circumstances you have to consider the loss of two generating stations caused by a loss of a large gas pipeline in a region or more than one region, so I have a couple questions about that, either for Mark, Dede or both.

One is are those the right entities to give us the kind of analysis and preparation that we need. You know transmission planners, planning coordinators, first of all, are balancing authorities who are the entities responsible for balancing resources and demand. Should they have some kind of responsibility like that?

And second of all, you know transmission

planners sometimes have a large footprint, but many of them do not. Some of them have a small footprint and having a lot of little entities, small entities do this analysis may not give you the necessary insight and results because a pipeline may affect several of them in a row and they each see only their tiny slice, which may not be the problem.

MR. SUBAKTI: So California ISO we're planning coordinators for the footprint that we have in California. You're right that I think, as a planning coordinator, we do see a lot more information with regards to how all the gas infrastructures ties into our portfolio.

One unique thing about California ISO is we are also the balancing authority, so because of the fact that we are planning coordinators and we are the balancing authority, we don't see that issue that you were talking about, but I would imagine if you are only planning coordinators and not a balancing authority you might have that issue. I would agree with you in there.

Currently, we are doing the assessment for the impact of potential gas pipeline in there because obviously again we've learned through it because we have Aliso Canyon's issue that is in there. I think we are in the right directions. We believe that there is a good -- at this point in time there's a good balance between reliability standard for the planning horizons versus what

commissioners have allowed us to do to have the market incentive to implement the constraints of the gas itself into the market optimization.

So it becomes a transparent step. Where do we need the renewable resource? Where do we need the other type of resource? Where do we need the energy storage and this other stuff, and I think the ability to have a mix of resources, mixed type fuel resources would help to reduce the over reliance on the gas. But obviously, this is one the things that has been a very good experience for us. And one of the things that we also have to look at, not just the planning of what would you if you have a pipeline that doesn't work, but then the question is what would you do if you actually have a blackout, a long-term blackout with a gas pipeline?

You know many of our black start resources are natural gas units, so we actually went through this exercise to look at which are the gas compressor that rely on electric simply to be there versus which are the compressor that are actually self-propelled that they can actually self-power through the gas itself. So that exercise is very useful for us.

MR. LAUBY: Thank you for your question, Michael. You're right there is a TPO I think, four, you know called for studying certain types of events, extreme events,

including the loss of a gas pipeline and especially if they impact more than one generator or a large number of generation. And the whole idea there is to develop plans to address those and then, of course, that moves into actually implementing some of those plans down the road becomes a closer scenario.

It's something to think about now, though, because it's becoming less and less of an extreme and more and more a shorter -- you know in our face type of event that we might want to look at that standard and see if it makes sense to have really into -- put the solutions in place, that one to five-year timeframe.

MR. BARDEE: A different topic, I have a question or two on EMP. One, Dr. Baker, I'll start with you, but others can feel free to chime in, has to do with let's suppose that some point in the future the Commission decides it's time to do a standard about EMP. It's time to require a standard about EMP. If I compare it to GMD, it's a natural event and you can put a number out there for GMD and say protect to this level and you don't have to worry about the sun reacting and saying I'm going to get bigger and hit the Earth harder, but if it's an adversary, a nation state or otherwise, if we specify a level of protection in a standard for EMP, is it a concern that adversaries may respond to that? Is that a risk?

DR. BAKER: I would say because of some of the limiting effects of the atmosphere, saturation affects we call them, that you can develop a bound that would be very difficult to exceed. For instance, we've done calculations in developing the DoD standard where we varied the yield by three orders of magnitude and noticed only a factor of 4 difference in the peak field. And so for E1, I think that's not a problem. For E3, again, it's very yield dependent, monotonically yield dependent, but we know what's in the stockpiles and so we could set our standards that bounds the E3.

The Europeans have the International Electric Technical Commission. It's already published some international standards, which, at least for E1, I think would be a very good one to adopt.

MR. BARDEE: And following up on what you just mentioned about the IAC, I've read there are standards there. There's the Mill Standard, MIL, from our Department of Defense, but I've also read that those are not generally developed with the grid in mind, may not be necessarily the best approach for the grid and also might be fairly costly if they were required. And I just wonder what your perspective is on that, whether those standards have some suitability or is there anything we can learn? Any part of them we can take and use here as sort of a no regrets.

Let's start with that.

DR. BAKER: Well, for the environment, you know DoD has all kinds of infrastructure and systems out there, so the environments are independent of that where it gets to be -- or the system affects in the grid and the grid itself comes into play is when you start talking bout coupling, but I think the environment standards you could develop some that would be universal.

DR. HORTON: So I would agree with the environment piece. I think where the difficulty comes in is you've got several things playing here. You've got the environment. You have the coupling piece, which would be the modeling aspects, but then you also have this piece, okay, you can sort of calculate what you think the equipment would be exposed to during a particular event, but would it be damaged? And then also what can you do in order to kind of mitigate that damage. I think that's where the questions for, for example, substation hardened equipment. There's questions around what would the equipment actually be exposed to and then what would the potential damage be. Once you know that, you can kind of back into what the mitigation options are.

Right now you know Mil188125-1 would assume that the equipment you're trying to protect is not very hardened at all, so it's pretty robust protection. So that gets to

be very costly, so what we're trying to do from our research perspective is, is there a way to still get the same level of mitigation because you're trying to harden different kinds of equipment and do that in a more cost-effective manner. But right now there's a lot of research to be done in order to get to that point.

DR. RIVERA: So if I could just chime in, I'm going to harp on this yet again. The answer to your question is workflow related. We don't have an accepted workflow. And when I say workflow that's not just a matter of, okay, these are the steps we do to get a quantitative answer, but that also is what are the bounds of what we are calling damage that we're concerned of?

Until we have that accepted workflow, until we have the appropriate bounds for what we're actually concerned about, we don't know which parts of the IEC standards or the Mill standards we need to pull out and plug in to the workflow to establish, okay, well this is the appropriate workflow and we can use this part of the standard, so it's workflow related again. Until you have a defined workflow, I don't I can't help answer you that question.

MR. BARDEE: So my last question before I turn to my colleagues or others, and your answer was actually a good setup for it. Let's suppose we get to the answer where

that workflow is now done, we know the answer. We know what we want to do. I assume there is a big, big difference in cost of installing it in something new you're building today compared to a retrofit of a substation or a control center or anything else that's big. And assuming that we have the flexibility to actually impose standards on new stuff without mandating the same treatment for old stuff, would that be a reasonable thing to do?

DR. BAKER: I would start there. And I've read that in the next 30 years we're going to have a 50 percent build out or increased build out in the grid, if that stat is correct.

The other point I would make is the DoD experience is that if you want to do global shielding for a new build versus a retrofit, there's a factor of 10 difference in the cost, 2 percent versus 20 percent it's roughly. But there are in some cases, for instance, in a substation control building you may be able to isolate the electronics in a very small volume, in which case the protection costs would be much lower. So there's ways to protect existing equipment, if you're clever, that would not obey that factor of 10 ruling.

DR. HORTON: Just one thing I would add, cost aside, I think when we start applying some of these hardening principles and practices in substations, I think

we've got to be a little bit careful about some of the potential unintended consequences, particularly when you start to look at applying HEMP filters to CT and PT circuits and things like that.

I'm not saying we can't engineer around those, but I think just kind of blindly applying some of the hardening could potentially cause issues that we need to vet out and make sure that's not a potential issue.

MR. ORTIZ: Thank you, Mike. Thank you all for your testimony and for the lively discussion.

I want to bring up just one question regarding an item that Tom Popik put forth in his testimony -- in his submitted comments rather. And this has to do with the notion of resilient versus non-resilient capacity, meaning simply that fuel is stored onsite. This could either be I guess a dual fuel facility with some fuel stored onsite or alternatively a coal-fire power plant or a nuclear power plant and there's a suggestion in the testimony or rather in the submitted comments that somehow we should come up with more effective ways of measuring and valuing that resilient capacity in some way.

And first of all, I'd like Tom to make sure that I didn't misrepresent his remarks and also I'd like the panel, perhaps Mark and others, to comment on that notion and potentially could be done about it, either here at the

Commission or within industry. Is it more than just smart black start planning? Is it something else beyond that? Help enlighten us on what potentially could be ways to think about that kind of resilient versus non-resilient, whether or not there's a valuable way of putting it. Help us understand that, whether or not that makes sense or that's something that could be a potential area for action.

MR. POPIK: I'll go ahead and get us started off because I would like to throw out some numbers about how severe the reduction in the resilient generation capacity has been. So just to reiterate what you said, if there's fuel stored onsite, the generation capacity is resilient to short-term interruptions in fuel supply. So this would be a hydroelectric plant, a nuclear plant, a coal-fired plant with a large coal pile or a gas-fired plant that has dual fuel capability that would have oil tanks that could run for, say, 24 hours or 48 hours, so that kind of thing.

And so what we did is we went to the EAI data and we looked at two different points in time. We looked at 1996 and we compared it to the most recent data available, which is 2015. So in 1996, 97 percent of U.S. generation capacity was what we would call resilient, that had some degree of fuel stored onsite.

And when we get to generation that's been added to the system, 1997 and later, on 27 percent is resilient,

according to that definition and in some states the reduction resiliency has been especially extreme. For example, in California only 7 percent of the newly added generation, which is almost entirely gas-fired, is resilient or dual fuel. And you can actually go around and visit plants and you can see the old oil tanks that no longer have fuel oil in them.

So what's the solution to this? It's very difficult to solve this problem with reliability standards. And this is where FERC has a tremendous advantage in terms of also being the economic regulator and being able to set certain conditions of tariffs. And so one of the things in our written tariffs testimony we suggested that perhaps there could be some adjustments to the capacity markets where there could be some allocation of capacity set aside for resilient or dual fuel type plants.

MR. LAUBY: Conceptually, I think I'm really quite comfortable with the definitions, remembering that NERC has been looking at this problem for quite some time. When we looked at the Clean Power Plan and how many plants were going to retire and what are the implications of being single threaded on gas and that's why we have a report on single points of disruption and pointing to what are the potential impacts. And in fact, in our LTRA, we're starting now to get to the point of saying, well, we want to

know how many of your plants are dual fuel? How many of your plants are buying on spot or firm so that we can start getting a real idea of the size of the problem, as Mr. Popik's pointing out and what are the implications on reserve margins. How we can get an expected value of gas for not being available? We can kind of play around with that. So from a planning perspective, the methods are there and then you can start looking at what the implications are and what the value to reliability is of each one of those resources.

MR. SUBAKTI: With regard to California ISO, we do look at our black start resource, black start capable resource carefully. And you're right there's specifically one black start resource that remain -- capability. There are quite a number of black start capabilities that are hydro-based, but there are also some that are natural gas.

Now for those that are natural gas, we have to go back and make sure when working with the gas company to look at whether or not the delivery of the gas would rely on the electricity. We want to make sure that they do not rely on electricity because they have to be on a compressor site that is self-working in there.

But beyond that, we have also worked with different technologies. So for example, we have a quick start capability from a HVCD line. Normally, HVCD lines are

not for black start, but we've worked with manufacturers, with Siemens and what not to have the ability to have a quick start for the area of San Francisco because, as you know, there is no more conventional generation in San Francisco, so we look for technology improvement.

The other one that is going to be interesting is that through the -- process in there one of the measures was try to look at the potential of coupling battery storage and be able to work and help to start some of the unit that may need to be quick start. So I think we have the right people to take a look at all the solution. Dual fuel maybe one of the solutions, but I think there are -- maybe there are other emerging technologies that could actually help us towards the solution.

CHAIRMAN LA FLEUR: I guess if there's one minute, I'll ask one more question while I have all these resilience experts. Something we've been hearing a lot about is analog backup. I know it related to cybersecurity, but it might relate to E1 and communications as well. Is that something you see as part -- you know that there's a King Risch bill and so forth and the thought of -- I have to admit when I first heard it I was originally kind of skeptical, but I've kind of warmed to the thought of some different modalities of communication or ways to run the system. Is that something NERC has looked at or thought

about?

MR. LAUBY: I know that like in the recent study that we did, the joint study with FERC on the loss of many of these are communication or situation awareness, and also we went through and identified some of the different types of communication methods. You can be using satellites and cellular. Of course, cellular could be gone to. It depends on how far you go. Pretty soon you've got a cup with a string on it, but I mean at some point you know have maybe microwave and other technologies that you can use. So it's an idea especially to practice these different types of drills and then really look at which are the most resilient communications that you want to count on.

CHAIRMAN LA FLEUR: Well, the companies used to have those -- what were they, megahertz systems and the trucks with the push to talk before the cell phones.

MR. LAUBY: Yes. So it might be worth having those on board. And I want to have people on each one of the substations. How are they going to communicate with those folks?

CHAIRMAN LA FLEUR: When you picture trying to put the grid back together, it seems handy.

MR. LAUBY: Yes.

MR. POPIK: There's one instance where retaining analog capability would be especially important and it's at

the large hydroelectric facilities. Those are almost entirely plants that were built, say, 40 or 50 years ago with original analog controls. Some of them have converted over to digital, but if the old analog controls are still left in place, and importantly, there's practice or drills using the analog controls that could make a much more resilient grid and that's, as you said earlier today, that's one of the key words, how do we ensure resiliency, and one of the ways is by keeping some of that old, resilient analog capability.

CHAIRMAN LA FLEUR: I mean that was a stupid example, but I'm sure everyone in this room has a manual can opener somewhere in their kitchen.

COMMISSIONER HONORABLE: I mean it never doesn't work. It always works. So whenever that electric one screws up, and it always does -- sorry, whoever makes them -- I go to that manual one.

MR. CLERMONT: But you're right. One of the paradox of what you're talking about is one of the driver behind going digital in our substation is the loss of expertise on analog. All our technicians that were born and worked for a long time retired -- with analog -- pieces are retiring, so that loss of expertise is something that we're concerned about and it's kind of giving an incentive to move faster towards digital. And Mr. Popik's right. I mean all

of use our network infrastructure was not built all last year, so we still have that, but we're losing fast the expertise on that, the spare parts, and everything and that's an incentive to go digital. But maybe we will revise that, revisit that in the future.

CHAIRMAN LA FLEUR: Thank you.

MR. BARDEE: With that, we'll wrap up this panel. I'd like to thank all of you for your time and for your very thoughtful comments. Thanks. And we'll be back at 3:15.

(Break)

MR. BARDEE: Our panel now is addressing the topics of cybersecurity and the CIP standards and other efforts that might be helpful in terms of better protecting the grid from the risk of cybersecurity. So I will start by turning to Marcus Sachs from NERC to lead us off.

STATEMENT OF MR. MARCUS SACHS

MR. SACHS: Thank you, Mike. Good afternoon. Madame Chair and Commissioner Honorable, thank you for having us and for the opportunity to appear before the Commission and staff and others to discuss grid security, also the work we're doing at NERC and with the electricity EISAC to mitigate potential impacts to the Bulk Electric System.

I think we all know that assessing risks and

assessing the security state is hard. It requires dynamic of constant vigilance and agility. The threats continue to evolve, particularly nation state threats as well as criminal threats and others as society changes and as the world dynamics change so do the threats, so that attention to detail, of course, is very important.

At NERC we address cyber risk through a variety of regulatory and non-regulatory means. Our mandatory CIP standards, which you all are very familiar, are our foundation for where we start with security. They provide universal baseline protections, but because that ever-evolving nature of threats standards alone cannot stand up to that challenge. We have to do other things. We have to have vigilance. We have to respond to these new and changing events.

We also have at NERC the Electricity Information Sharing and Analysis Center or EISAC, which serves as an information-sharing conduit, which when the electricity industry and the government for cyber and physical threat exchange threat analysis and understanding what's happening.

The EISAC facilitates communication of important or actual information and we strive to maintain what we call the ground truth, the actual information about this rapidly evolving security world. Together these mandatory

standards, effective information sharing, working together provide a very robust and agile toolset to help us protect the Bulk Power System.

In addition, we also work very closely with our partners at the Electricity Subsector Coordinating Council or the ESCC, very unique to our sector to have the CEOs involved in security discussions and I think we have a very, very, very strong public/private partnership that's important to addressing this security world.

Let me just briefly walk through what we see as -- and the EISAC has learned a lot about security over the last couple years as we continue to grow and change, but there's probably five major areas we're concerned about that the grid needs to worry about and this is just cyber. I think we all understand the physical challenges that are out there, but we see a lot of cyber stuff that began years ago with more of a reputation problem protecting websites -- you know phishing, stealing domain names. That's an inconvenience problem, but I think it's something that as long we're very aware of it and we're tracking, certainly it's something we can handle.

But we've also seen the criminal world move into theft, both theft of intellectual property as well as theft of value. This is the old FBI thing -- you know why do you rob a bank. It's because it's where the money is. Well,

the electric grid is not a bank like financial services, but we have a lot of value and we're certainly seeing a large rise in cyber crime. And it manifests itself probably in two different ways. One is the stealing of customer information, credit cards, other things. The other would be this new wave of ransomware that we're seeing. You're all are very familiar with the Wannacry problem that we saw globally about a month or so ago.

Again, that area, that theft of information and theft of value as well as reputational theft, those are all things we can understand. We can mitigate. It's a nuisance problem. But where we get into the stuff that really worries us with the grid is that folks are able to cross a boundary and begin to manipulate control systems. That is the growing concern area. It's largely been theoretical, but we've seen through the Ukraine incidents and others that the theory is now becoming practical and our adversaries are very interested in some of the successes that they've seen.

We've done quite a bit of studies and have released a number of white papers and have worked very closely with others in our sector, many who are sitting here, as well as other industries to better understand and analyze what's going on. The worst case, of which we've got very few examples, is beyond just disruptive like what we've seen in the Ukraine, but destructive where you have an

adversary get in and actually break things, either logical destruction causing the devices where they can't respond to commands or physical destruction, such as spending device, which the (0:04:37.1) Group had uncovered with Aurora many years ago. I don't want to say that's right around the corner, but that seems to be the next wave and that's where we really need to be vigilant when it comes to cybersecurity.

So I've got quite a few remarks in my written testimony. I encourage conversation and questions. Look forward to a vivid discussion as we move forward. Thank you very much for the opportunity to be here today.

MR. BARDEE: Thank you, Marcus. Next, we have Dr. Manimarun Govindersu, from Iowa State University.

STATEMENT OF DR. MAINARUN GOVINDERSU

DR. GOVINDERSU: Good afternoon. First of all, I express my sincere thanks to the Commission for providing me this great opportunity to be part of this panel. I'm a professor at Iowa State University. I conduct research in cybersecurity for the electric power grid.

As you know, modern grid is a complex cyber physical system with incorporation of smart sensors, communication networks, various controllers. They've improved. They appreciate the availability and the economics of the grid, but they're also increased the

attacks and risks of the grid for adversaries to exploit, so we need to secure those attacks and risks. We need minimize the attacks and risks.

So in recent years, the cyber threats have been growing in numbers, also in sophistication. We know of several incidents in recent years in the Ukraine and other places. The legacy nature of the grid, coupled with the slower adoption of operation technologies makes this problem even harder.

So in this context, I would like to identify a few R&D challenges and also they are related to policy as well. One important thing is we need a holistic cybersecurity framework that encompasses attack, deterrence, prevention, detection, mitigation, resiliency and forensics. We need to have a holistic as opposed to a comprehensive framework. That also has to accompany with property at the realistic metrics and tools and they are to be operationalized and realistic environment.

The other important thing is risk assessment has been talked today. The current cyber assessment is more qualitative in nature as opposed to quantitative in nature. And also they do not properly account the threat tactics. If you look at risk assessment, risk involves threat times vulnerability times the consequence. Threat modeling is not well understood. It is more of an art than a science today,

so we need to better understand threats so that we have more realistic risk models for cyber threats.

The third important thing is the current notion of resiliency is a fault resiliency which has the notion of N minus one contingency criteria. How do we transform the current fault resiliency to attack resiliency to deal with malicious adversaries who target multiple critical elements -- coordinator attacks and so on. So paradigm shift from fault resiliency to attack resiliency is important.

The other one is the innovation in IT outpaces the operational technologies. There is always a catch up in OD trying to catch up the IT. The adversaries have advantage because they use IT tools and technologies. How do we bridge this gap is very important. NERC compliance has been very effective over the years. Continuous improvement is important. While we make this continuous improvement, it has to be to the extent very fine, the effectiveness of the process, the technologies, and the people who operate the system they all have to encompass what has been in place. The challenge has been how do we sustain it? The industries find it hard many times how to sustain this compliance process.

The other important thing is how do we extend supply compliance to distribution grid. Distribution grid is not well -- or well protected against cyber adversities.

That needs careful attention. Grid exercise has been growing in terms of industry participation and sophistication of the scenarios. There is a need to incorporate test-based experiments in grid exercise scenarios.

Finally, workforce development is extremely important. As I come from university, we imparted graduate education, undergraduate education, industrial training, hack-a-thon and so on. There are so many flavors of education that can happen in which industry, university, and federal agencies can collaborate together.

So finally, synergetic partnership among industry, universities, and federal-funded national labs is important, not only to advance the R&D in this important area, but also to educate and train skilled workforce in a sustainable manner for the future. That concludes my remarks. Thank you again.

MR. BARDEE: Thank you, Doctor. Next, we have Michael Assante from the Sampson Institute.

STATEMENT OF MR. MICHAEL ASSANTE

MR. ASSANTE: Good afternoon, Chairman LaFleur, Commissioner Honorable, and staff. I thank you for this opportunity. I'll summarize my remarks for brevity.

In addition to my experience as a CSO at AEP and the first CSO at NERC, I'm providing these comments based on

my recent experiences with real world incidents involving power systems and my understanding of the opportunities and challenges developing industry standards.

I remain steadfast in my belief that properly developed standards play an important role in establishing a very strong foundation for future electric system reliability and security. It is important, however, to recognize that the standards cannot be formulated to fully protect against all possible manifestations of future cyber intrusion and attack.

The NERC standards have grown considerably in both scope and effectiveness over their 14-year history. While much has been done, there remains much to do. There will always be a regulatory lag between the CIP standards and current cyber threats. Acknowledging this lag, there should be a focus to enhance emergency operations and incident response requirements.

In this way, even if the standards do not specifically require a control or mitigation for unknown attacks of the future, the standard would still provide guidance to facilitate a response and recovery. For these reasons I believe additional modifications to CIP008 and CIP009 should be a priority for industry consideration. For example, required communication with the EISAC upon identification of a potentially impactful incident rather

than upon an actual impact to a reliability service would provide earlier visibility in an effort to protect other utilities.

The requirements as they are today would be comparable to a medical professional not sharing the results of your routine medical tests or cancer pre-screening for your awareness and early action, but instead waiting until you had organ failure to alert you that you have Stage 4 cancer. The requirement is written at such a high bar that few conclusions can be made or taken from the lack of reports that we see.

Also, we need to learn from other NERC reliability standards. I believe the standards need to mature in three ways. One, require a similar level of competency demonstration for the cyber defenders or cyber operators, if you will, at the Bulk Electric System. Two, acquire a level of response knowledge and capability of the certified electric systems operators, ensuring an understanding of appropriate responses to their systems being misused. And three, develop the operating protocols, tools, and capabilities to rapidly ascertain the risk of continuing to operate parts of the system containing attacks and developing approaches to measure the integrity of systems if they're being returned to service.

There are many lessons to be learned stemming

from the 2015 and '16 Ukraine incidents. We need to move beyond the question of whether similar attacks is possible in the United States and instead shift our focus to mitigation and response requirements with the expectation that a similar or even more impactful attack could occur here. Continued efforts from NERC focused on utility exercises like Grid-x and Dewey-lead industry workshops and private sector provided technical hands-on training will continue to improve our overall capabilities and preparedness.

This is a very encouraging area where I believe NERC registered entities are moving far beyond the requirements in the standards. Recently published reports examining the 2016 Ukraine cyber attacks targeting their country-wide transmission system operator, paint a picture of an evolving threat. Analysis of the malware describes a tailored tool for the purpose of causing electrical outages. The flexible and modular tool possesses features that aid the time in collapsing the time it takes to complete the necessary steps to device and launch an attack that can disrupt operations and potentially damage infrastructure assets.

Also, it appears that the attacker interest in system protection has moved from information gathering to developing an initial capability to exploit both control and

protection. Threats like this demonstrate that we must empower defenders with defensible environments, which the standards do. To this end, though, industry also must have the latitude to experiment and field new prognostic and security technologies that can change the pace to catch up to cyber attackers.

As an example, the Idaho National Laboratory and industry partners are further building upon the industry's great strength by developing engineering-centric assessments and mitigation methods called Consequence Driven Cyber Informed Engineering. The goal of this program is to actually engineer out the worst cyber risk that the energy infrastructure faces.

Finally, public reports of successful broad axis campaigns and modular toolkits may indicate attackers are becoming more focused on attacking larger numbers of devices to cause widespread impacts. The positive evolution of CIP standards have provided more protections to a greater number of systems and this may need to continue.

So with that, I thank the Commission and staff and look forward to our discussions.

MR. BARDEE: Thank you, Mike. Next, we have Greg Ford from the Georgia Systems Operations.

STATEMENT OF MR. GREGORY FORD

MR. FORD: Good afternoon Madame Chair,

Commissioner Honorable. I appreciate the opportunity to participate on the panel on behalf of NRECA and our member cooperatives in Georgia. There are no single standard requirement that stands out as the most effective cybersecurity control. Instead, I believe it is the interrelated nature of the controls that together provide a defense in depth posture that makes the NERC CIP standards effective.

The key aspects of CIP Version 5 was the introduction of the cyber system impact categorization, which has expanded protection to the entire Bulk Electric System while acknowledging that not all facilities have the same risk profile. While I have noted that standards work together as a whole, it is important to point out that Version 5 introduced controls that are consistent with a key lesson learned from the Ukraine event. CIP Version 5 requires that all interactive remote access first pass through an intermediate system and leverage multifactor authentication.

In addition the CIP standards, internal controls that the industry is adopting ensure compliance and more aggressively mitigate security risks. We have internal controls not only for CIP operations, but also for other Bulk Electric System operations. We have embraced internal controls as a part of our day-to-day operations to help

avoid mistakes and prevent cybersecurity breaches. At GSOC, board-approved corporate goals measuring the implementation and testing of these internal controls are a component of our employees performance pay.

We urge restraint on pursuing new mandatory CIP standards. We are still in the first year of CIP Version 5 and have not yet completed the implementation of some requirements for low impact systems. Time is still needed to fully implement these standards and absorb the lessons learned from this implementation.

Further, we need to avoid thinking that mandatory standards are the only path to improve security. We believe that voluntary recommendations and actions should lead before the mandatory standards because they are faster to implement and more flexible to change. Organizations such as the EISAC are well positioned to coordinate voluntary recommendations to the industry.

We also recognize that as the cybersecurity field continues to mature new technologies will be introduced that could improve the overall security posture of the grid. These new advanced security technologies will no doubt come and go. By the time the new technology can be incorporated into a mandatory standard, it may no longer represent the state-of-the-art. The approach moving forward must ensure that a solid security framework is in place, but

also enable us to be nimble in the face of an ever-changing threat of our landscape.

During the first year of mandatory compliance, we learned that some standards are taking a disproportionate amount of time to execute. In particular, we highlight CIP 7 and CIP 10 baseline standards. While we certainly recognize these standards are important, we believe that improved security could be achieved if they focused on having adequate controls in place to achieve the security objective rather than specifying performance details.

For instance, the current patching requirement dictates a specific process across all devices to assess and implement security patches within a detailed timeline. An alternative approach could be to focus on the security objective of implementing a flaw remediation and vulnerability management program with the flexibility to recognize different areas of risk and apply resources accordingly.

As our industry expands a culture of internal controls, we need to continue to move towards an environment where the focus of the oversight is on ensuring that controls are in place to monitor and maintain compliance and security. In this environment, deficiencies that are detected and corrected by a company's control should not result in a violation.

The Electric Subsector Coordinating Council is a key coordination point between the electric sector, the government, and other critical infrastructure, such as telecommunications, oil, natural gas, financial services, transportation, and water. The ESCC is working coordination with the EISAC to bring these sectors together to improve cross-sector awareness and facilitate cross-sector exercises. The upcoming Grid-X4 exercise is just one example of how the electric sector is committed to improving the resiliency and ensuring cyber preparedness.

In conclusion, we appreciate the focus and the effort of the Commission to improve the security posture of the grid. The existing CIP standards mandate that necessary elements of a solid foundation cybersecurity program and have contributed significantly to the improved security of our system.

I'd like to thank the Commission for the opportunity to participate on the panel and I look forward to questions. Thank you.

MR. BARDEE: Thank you, Greg. Next, we have David Ball from AEP.

STATEMENT OF MR. DAVID BALL

MR. BALL: Good afternoon. On behalf of AEP, I'd like to thank the FERC Commission and staff for the opportunity to speak on this topic.

AEP applauds the efforts of the Federal Energy Regulatory Commission in assembling this technical conference on a topic so crucial to the reliability of our nation's electric grid. AEP is one the nation's largest electric utilities delivering electricity and customer energy solutions to nearly 4.5 million customers in 11 states.

AEP owns the nation's largest electric transmission system with more than 40,000 miles of network transmission facilities. We operate 224,000 miles of distribution lines and rank among the nation's largest electric generators with 26,000 megawatts of capacity, which includes 3200 megawatts of renewable energy.

Cybersecurity, like all security, issues is of paramount importance at American Electric Power. We have a robust cybersecurity program at AEP, one that is under continual evaluation for process improvements. We are in constant contact with our state and federal regulators and our regional reliability entities to ensure that we are current on all threats that face us so we can institute the best possible protections.

AEP would like to thank FERC and NERC for the standards created and enforced in the area of cybersecurity. The standards serve as a starting point help drive a common framework for the cyber and physical security protections in

which AEP engages. The checklist of NERC standards is a solid foundation, but if we were to engage in those activities and nothing more our Bulk Electric System could be seriously at risk.

AEP engages in many voluntary actions to improve both the overall cyber and physical security of our system that is part of our large Bulk Power System. These are precautions and protections we implement because they are the right thing to do.

You asked about specific protections and asked us to relate our practices to internal crisis that have arisen in the past few years, most specifically, the attacks on the Ukraine electric grid. Speaking to the 2015 Ukraine cyber attack, security regulations already in place in this country would prevent such an attack from occurring here. The attackers in the Ukraine incident infiltrated the cyber systems and observed work patterns and practices for months before seizing control of the Ukraine grid. Their efforts were enabled by the fact that the business systems and operations systems were integrated. This mixing of functions violates U.S. regulations.

Because our systems are separate, an attacker could not hack into the business functions of U.S. grid operations as a means of access to operational systems. For example, standards for patching, configuration, change

management, and malicious code prevention have driven industry to implement a framework of controls to protect our critical system from vulnerabilities and exposure to cyber attacks such as Wannacry attack in May of this year.

The CIP standards also have helped in restricting communications in and out of our SCADA networks, which we saw exploited in Ukraine in 2015. Also, we require intermittent systems and multifactor authentication to ensure only authorized personnel and communications can access our SCADA network.

We need additional transparency and consistency in the auditing process. Currently, different regions view standards differently and we sometimes are challenged by those inconsistencies as we strive to meet the demands of three regional entities. Additionally, when problems are revealed during the auditing process those issues need to be transparently outlined in an audit report issued by the regional entity. Transparency and consistent terminology in communicating violations would greatly enhance the benefits of these audits.

Another area to consider related to consistency is our frequent standard revisions. This presents a risk as the resources needed to improve and maintain cybersecurity often are consumed with keeping compliance processes up-to-date to reflect standard revisions. For the past two

years, the industry has been advocating for increased screening processes for new hires in the cybersecurity arena. Currently, background checks are conducted by third-party vendors using publicly available data.

To increase security of the grid, we should be able to access fingerprint records housed at the Federal Bureau of Investigation. This would not necessarily need to be a standard practice for utility new hires, but could be restricted to those working in critical infrastructure and Bulk Power System positions. The industry would benefit greatly from the Commission's support in this endeavor.

In conclusion, I would like to reiterate that AEP is fully committed the security of the electric grid as discussed above, consistency and transparency and NERC requirements would help facilitate our compliance, support from the Commission as we advocate for FBI assistance in background checks of new employees would be helpful, and strong communication and relationships between the Commission and the states would be beneficial as we work to ensure the security of the grid.

Again, we appreciate the opportunity and I look forward to your questions.

MR. BARDEE: Thank you, David. Next, we have Nathan Mitchell from APPA.

STATEMENT OF NATHAN MITCHELL

MR. MITCHELL: Thank you. I want to thank the Commissioners and FERC staff for inviting me to participate in this technical conference on grid security. I am here representing the over 2,000 municipal and state-owned electric utilities that make up public power.

I would like to remind the Commission that APPA and its member utilities have supported the work of the industry-led standard drafting teams in their efforts to develop risk-based standards through the NERC standard development process. These standards provide a needed baseline of cybersecurity controls to protect the Bulk Electric System; however, we cannot continue to write new standards to address every threat. APPA believes that the CIP standards need to reach a steady state.

We are encouraged by FERC staff's recent request for input on how standards can be made more efficient while maintaining their effectiveness. APPA stands ready to assist the Commission with its request to right size the standards to make them less burdensome on industry.

Please don't take my suggestion as an indication that we should not continue to protect our system from ever-increasing cyber threats. I believe that more can and should be done to address the cyber risks to electric utilities, but these efforts should be focused on voluntary programs outside of the NERC standard development process.

I would like to highlight one voluntary program being developed to help public power utilities address cyber risks.

As I provide a description of these efforts, the Commission should recognize that it meshes with other industry, government, and university efforts discussed by my follow panelists and to make up a community approach to cybersecurity. APPS has partnered with the Department of Energy to undertake an extensive, multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities.

In this project, APPA is providing public power utilities with an array of security tools, technologies, and programs so that the community is better able to understand, install, and implement new cybersecurity programs. Importantly, this project will bolster the programs for many small utilities that do not own or operate bulk electric system assets and thereby, not registered with NERC.

First, we have developed a simplified maturity model as a tool for small utilities to understand the characteristics of a mature cybersecurity program. The maturity model will help public power utilities enhance their cybersecurity program based on their organizational structure risk profile. The project has begun to evaluate information-sharing tools and technologies that will improve

threat information sharing between utilities and the EISAC. Recommendations will be developed on how best to characterize, assess, disclose, and disseminate secure threat information that is useful and useable for public power utilities.

And I believe that workforce development is essential to ensuring that public power utilities have the proper human resources to manage their cybersecurity programs. Public power utilities often face difficulties in identifying and recruiting qualified cyber and physical security candidates due to their location and/or size. Working with universities, community colleges, and other educational and training institutions across the nation, we will explore the development of educational programs that meet the staffing needs of a typical public power utility. We will then evaluate if online opportunities can be developed so that they can be easily accessible to remote communities.

I look forward to the comments of the other panelists on how we can educate our current and future workforce to address these cybersecurity challenges.

Finally, the industry needs a robust cyber incident response plan. APPA plans to develop a model playbook which will address potential roles and responsibilities within small public power utility to

respond to a security incident. In many small utilities, one person has many roles and responsibilities. As such, a step-by-step playbook on what actions to take first, who to coordinate with, and other types of response activities will supplement existing natural disaster mutual aid programs.

I refer the Commission to the other industry incident response playbooks, such as the one created by the Electricity Subsector Coordinating Council, as a model for the public/private partnership needed to respond to a national level event. I believe that APPA's voluntary cybersecurity program will help improve the overall cybersecurity posture of public power utilities and the Bulk Power System.

I appreciate the opportunity to provide these comments and look forward to your questions.

MR. BARDEE: Thank you, Nathan. Next, we have Commissioner Robert Scott from the New Hampshire PUC.

STATEMENT OF COMMISSIONER ROBERT SCOTT

COMMISSIONER SCOTT: Thank you. And Chair LaFleur and Commissioner Honorable and staff, I appreciate the opportunity to speak. It's always good to see you again.

I speak today as a Commissioner for the New Hampshire Public Utilities Commission. In one week, I will be the Commissioner for the Department of Environmental

Services for New Hampshire; however, I want to make sure that the Commission is aware, recognizing the importance of the work that's been going in New England. The governor's asked me to also act as the special advisor on critical infrastructure for cybersecurity, so in the context of no good deed goes unpunished, I get to do that work also. So in that context, I hope to still be able to engage with you and your staff.

Again, speaking as a state regulator, I also wanted to thank you for allowing and bringing the state perspective to this panel also. I think that's an important one. And I'll state the obvious, at least from my point of view. Obviously, the Bulk Electric System is very important to us all. However, as I'm sure you're aware, that the distribution systems also present a threat to the Bulk Electric System, so we need to work together in that capacity. Or to put it another way, obviously, NERC and FERC regulate the wholesale side of things, but unless the state regulators are involved in an effective way and the distribution utilities are involved in an effective ay I don't think we get where we need to go. Certainly, any artificial boundary like that is not going to be recognized by the adversaries that we're looking at for cybersecurity.

Our experience in New England demonstrates this interdependence. What we found is in working with our

partnerships that we've developed cybersecurity for our largest distribution utilities and the transmission owners are basically one in the same, so they're centrally managed, rightly so. It's generally the same staff and the same systems, so it's very hard, at least in New England, which I don't think is that unique to differentiate the two nor should there be.

In that context, I have some recommendations to point to, based on our efforts in New England. First and foremost, is the important of partnerships, we partner with the National Guard in the region, with the Department of Homeland Security, particular, the INA side of DHS. Certainly, FERC, the Office of Energy infrastructure Security has been a great asset for all the states, ISO New England, and to a lesser extent the FBI and Department of Energy.

I'll highlight. We've talked in your supplemental notice and some of the other panelists have talked about the Ukraine incidents that are going on, which are very concerning. Another incident which raise light in New England and thankfully it wasn't -- I don't want to say it wasn't real, but it was over -- incorrectly reported it was Burlington Electric situation.

That highlighted to me anyways as a state regulator the importance of those partnerships and the

importance of having relationships already. So we had in that situation -- I'm not going to characterize it as good or bad, but we had a governor make some very strong statements. So the governors need to know what to say and what's going on. I know, for me, I received a call. I was shopping Saturday morning and I got a call from the governor's office what's going on. And thankfully because we have these partnerships I was able to say I've already been in contact with these people. They're on the phone now with EISAC and yes, it's all under control. We're good to go. Those things are important to states.

So the other part of that, and again the Burlington Electric incident provided a good insight for the need of this is we need to exercise these things. So again, FERC, OEIS has developed some checklists that helped with the states in New England that we've been looking at. That has now set us up so that we can now start to conduct some exercises. So again, you don't know what you don't know until you start going through these types of scenarios.

Last week, with the National Guard, we had state regulators. FERC had staff there. New England Utilities, ISO New England were all participating in the New England National Guard Cyber Yankee Event, so that was yet another way you taking it to the next level of working together and understanding each other.

Another point I'd like to raise is security clearances. As the Commission's aware, a few years ago New England was in a very unique position as we had three state commissioners from three different states, myself included, with top secret or above clearances and we knew how to spell the word "cyber." So in that context, we were able to have discussions with the intelligence community, with our partners in Kansas, among others, as well as to start to talk to our utilities on the importance of collaborating on a classified level.

That resulted in New England of we've actually hosted in New Hampshire. We've been able to host a meeting of those obviously appropriately cleared to bring utilities and regulators in so that they could share information with each other, talk about common experiences at that level. That's something they haven't really been able to do in the past with that. Also, this experience has also allowed us to start to work to get higher level clearances for appropriate utilities, so we feel that's an important consideration moving forward.

Workforce development, again, New England's been taking a regional approach, understanding that we're all interconnected, especially in New England. The State of Maine, as part of our regional effort, is actually hiring a gentleman July 3 who was working with Cyber Command. He's

retiring. He has the credentials and clearance, et cetera. He'll be working certainly as a State of Maine employee, but he'll also be a regional asset to our efforts.

Having said that, that's kind of a work around what I think the Commission surely understand. At the state level, we're generally not staffed for these types of things. We don't have the expertise. We have accountants. You know we're here to be -- regulators and this is a new ground for us. So NARUC's done some groundwork, which has been very helpful, but that's something else that continues to need -- I think will need help because I don't believe this issue is going away.

Finally, again, I want to put a shout out to the FERC Office of Information Security -- Office of Energy Infrastructure Security. They've been a really great resource for our states and if we've called they've been very responsive to us, so I want to throw that out as a best practice. Perhaps other agencies could do the same.

So with that, I'll close my remarks.

MR. BARDEE: Thank you, Commissioner. And Brandon Wales from DHS.

STATEMENT OF BRANDON WALES

MR. WALES: Thank you. Good afternoon, Madame Chair, Commissioner Honorable and assembled staff. Thank you for the opportunity to address you today on behalf of

the Department of Homeland Security National Protection and Program Directorate.

MPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. And within MPPD, I oversee the Office of Cyber and Infrastructure Analysis, whose mission is to provide analytic support to our collective efforts to strengthen the security and resilience of our infrastructure and respond and recover from natural hazards and manmade events.

My testimony today will focus on two issues of interest in response to the questions posed to the panel. The first issue covers the need for traditional electrical utility planning activities to embrace cyber-base contingencies and the second issue focuses on the efforts of the Department of Homeland Security to increase and enhance information sharing and analysis activities with the electric sector.

First, as electric utilities adapt and increase their use of industrial control systems to automate and increase the efficiency of operations, cyber-related consequences of adoption of new practices and procedures should be carefully studied and evaluated to understand the potential impact of their loss or disruption to reliable operation of the electrical grid.

Cyber hazards do not have as well characterized likelihood and consequences to critical infrastructure assets and systems and cyber events can simultaneously occur over large geographic areas without respect to traditional boundaries of electric system operation or control. These events will stress traditional emergency management and response procedures designed to contain and constrain system problems.

To understand potential system impacts, a natural evolution may be for system planners to create a number of cyber contingency cases which could incorporate a variety of cyber threats that could affect system monitoring or communications and affect infrastructure operations. Cyber scenarios should have characteristics distinct from current hazards to challenges the utility's understanding of the degree of the impact possible from cyber events.

Second, the Department of Homeland Security works with partners at all levels of government and from the private and nonprofit sectors to share information and build greater trust to make our cyber and physical infrastructures more secure. This includes sharing information through platforms such as the Critical Infrastructure Advisory Council, the Electric Subsector Coordinating Council, and the Department's Physical and Cybersecurity Operation Centers, the National Infrastructure Coordinating Center,

the NIC, and the National Cybersecurity and Communications Integration Center, the NCSCIC. Information released by the NCSCIC and NIC maybe subsequently shared to the electric subsectors, owners, and operators through the Electricity Information Sharing and Analysis Center.

One of DHS's most prominent initiatives to enhance information sharing between the federal government and private sector that I would like to highlight is called Automated Indicator Sharing. AIS connects participating organizations to a DHS management system at the INCIC that allows bidirectional sharing of cyber threat indicators, helping to build the common, shared knowledge of current cyber threats.

AIS is a part of the Department's efforts to create an ecosystem where as soon as a company or federal agency observes an attempted compromise the indicator will be shared in real time with all of our partners, enabling them to protect themselves from that threat. This means adversaries can only use an attack once, increasing their costs, and ultimately reducing the prevalence of such attacks.

Another initiative to facilitate information sharing is the Cyber Information Sharing and Collaboration Program, which enables the sharing of cybersecurity threat information in a secure fashion with entities across

critical infrastructure sectors. CISCP, as it is called, provides for analytic collaboration between DHS and participating entities, and when appropriate, allows participating entities to embed analysts on INCIC watch floor. These efforts are designed to feed and complement energy sector initiatives that were highlighted in Mark Sachs' written testimony.

Future cyber events may not directly target electric power owners and operators, but may impact connected infrastructure systems, which the Bulk Electric System depends to ensure reliable operations. As our information technology systems become further interconnected and interwoven, disruptions will no longer be limited to a single infrastructure asset or system with consequences potentially far-reaching.

The issues I have raised here today are complex and don't lend themselves to the easy, silver bullet solutions. The Department of Homeland Security is committed to working with FERC and our partners in the electric sector to begin working these and other challenges facing the systems that power our country.

Thank you and I look forward to your questions.

MR. BARDEE: Thank you, Brandon. We'll start our questioning with Commissioner Honorable.

COMMISSIONER HONORABLE: Thank you, Mike, and

thank you gentlemen for your perspectives. I have a lot of ground I'd like to cover, but first I'd like to start by thanking each of you for the value you bring to this important work and I think we end it on an important note about focusing on the importance of this work and how much more challenging it was.

I remember, and I've been hearkening back to my state regulator days, but I remember we had a physical attack on our grid and that was my first encounter with the Joint Terrorism Taskforce and the friends that we have at the Department of Homeland Security thank you for your work. And I was able when I NARUC president to participate on the Electric Subsector Coordinating Council.

Also, Brandon, your colleague, John McClain sends me your daily updates, so thank you. I am well informed about the world of cyber, but it's a shame the state of affairs these days requires that, but it absolutely -- going back to Marcus's point, requires our vigilance that we're aware and that we're equipping ourselves with the tools to lead and to lead well.

Bob, I mentioned earlier today for our work with our state colleague, thank you. And I recall when I signed up to be a Commissioner, and I know it's the same for you; you had no idea about all of this part of it. And now you're going over -- thank you for your service -- to

another job and the governor's managed somehow to get you to do both at the same time. Thank you for saying yes because this work is so important. And men and women who have your experience and expertise are few and fair between, so thank you for saying yes. Your state colleague, the region will benefit, but also we will as well. So thank you for coming back for more.

I'm really pleased to end with this session because I think your perspectives have really covered the gamut of the fact that we are all working so hard on a number of aspects of grid security.

And I want to start with, Marcus, you talked about -- and thank you for your discussion about the threats and how different they are and it's important that we not lump all of them into one. We tend to talk about cyber generally when there are a number of aspects about that work that we need a singular focus.

But you spoke about ransomeware and disruptive threats. I wanted to focus on the crash override malware because you all recommended steps that utilities need to take to protect themselves and I appreciate your work along with DOE and our Office of Energy Infrastructure Security to really study what occurred in Ukraine to make sure it doesn't happen it here, and if we do have a threat or an attack, how we can quickly rebound. And I want to ask you

to just highlight some of the challenges that were presented by this malware and the strategies that we can employ to fend against that.

MR. SACHS: Thank you, Commissioner. That malware was interesting. First, we were not aware of it in the United States until a Friday and others were aware of it maybe two or three weeks earlier and it was not something widely known by any means. But do a good, strong public/private partnership on a Friday afternoon many of us working the weekend were able to get information out on Monday morning.

The group that discovered it in Europe had already planned to do a release to the media on their own. That group found a group in the United States, another private sector organization. They asked them would just please review what we're doing to make sure we're not saying anything technically wrong. That U.S. group said, well, if you're going to go live in the media, we need to activate. You know put up the bat sign to get people involved, so it was a very strong effort that just came together because the partnerships were in place. That if we didn't have those partnerships already existing, we would've failed that weekend and you would've had a media splash on Monday morning that none of us would've been ready for.

So the malware itself I don't know that we

necessarily need to focus on the ones and zeros of the malware.

COMMISSIONER HONORABLE: We don't. I just want to get your takeaways about it.

MR. SACHS: Absolutely. And I think there's so much more to learn about our adversaries. So when this malware was found, it is showing us new techniques, tactics, and procedures, or TTPs that again are long and theoretical, but now we're actually seeing it in software where an adversary who can build a modular tool, as we like to call it. It's almost like a Swiss Army knife. You've heard that analogy used.

COMMISSIONER HONORABLE: Yes.

MR. SACHS: Where this thing can be customized for different types of targets. It can lie resident undetected. It looks like regular software, but yet, it has a little evil bit to it. So instead of looking for signature, which is our typical way of looking for it, strings, ones and zeros, IP addresses, we now need to look more for behavior-based signatures. Things that aren't working like they're supposed to, which then requires a much deeper knowledge of what is it supposed to be doing, what is baseline, what is normal, and then being able to recognize what is not normal and then quickly determining is that a human error causing it to be not normal or is it something

we don't understand, which then they say, oh, we have a cyber problem going on.

And so this is going to require again another level of thinking versus just looking for signatures and malicious code, which is what we've really been doing a lot of and we're getting good at it, but it doesn't stop there. Again, I was thinking about agility. We have to keep rethinking how we think about security.

COMMISSIONER HONORABLE: Indeed. I don't know if anyone else wants to chime on that point, but if not, I will move onto the next one.

In thinking about your point about the partnerships, and it's similar to what Bob Scott mentioned about the call he got and because of his networks he was able to respond quickly about what was occurring, I want to emphasize the global nature of this work. Thank you for mentioning that.

I often say energy is global. That's why our work and why we invite our international colleagues here. We're working on the same issues. We're working on the same challenges and in particular in the grid security space, in the cyber space that's especially important. So I thank you for cultivating and nurturing that climate.

And to Bob Scott's point about lessons learned about that Burlington incident, I wanted to say that, yes,

we learned the importance of being prepared to respond, as Marcus just mentioned, being prepared with what we need to say in the media and what we don't. But another thing is something you mentioned and that's ensuring that we have a strong partnership. And I think, honestly, and I'll say it, for our part in the federal government we had some missteps too in that incident. And I think we can all learn from that and our goal should be inspire and strive for trust and for our ability to work well at all times. So I appreciate that you were candid about your takeaway. I want to be candid about us too, so we'll have to learn to trust and protect when industry provides us with information voluntarily that we keep it, as we should and as we've promised.

I want to turn also to the workforce question. Greg Scott and Mr. Ball thank you both because you've talked about workforce strategies.

Greg, you spoke about performance-based metrics with compensation. Hello, that gets everybody's attention. You start messing with my money, then I'm going to pay attention and what the hoops I have to jump through. That's important. And I want to ask others if you have grid security related performance metrics in your places of work, so think about that.

But also, David Ball mentioned your workforce

component as well and I want to tell you both how much I appreciate that. It's more than just us going to meetings and giving speeches and hearing lectures and reading studies. This is about making sure our men and women are trained because we're only as safe as the weakest link. That applies to our facilities and it applies to manpower too, so I was very pleased about staff's question for you. What can the Commission do to facilitate or encourage a strong cyber workforce?

I think about that internally. What are we doing to make sure that our staff is trained? We have trainings that focus on not clicking through on that darn thing we know we don't need to click on? What does that also elate to with regard to hiring the best? That's a great story about Maine snagging the gentleman that's retiring. Those folks are few and far between as well.

How can we ensure in the same way that we're hiring the best market operators, transmission planners, that we're hiring skilled people who are equipped to help us secure the grid? So two questions, one is about your strategies where you are about making sure that grid security is a priority and then what are you focused on externally for hiring talent.

And I think we're getting feedback, so if you aren't speaking, please turn off your microphone. Thank

you.

MR. FORD: Thank you, Commissioner Honorable, for that acknowledgement on our performance and how we handle things. When we started with this route 10 years ago, of course, security and reliability is important to us all. It was very important to us as we saw this culture changing we wanted to try to get ahead of it and we felt like there was no better way to get people's attention and get the culture in the right frame of mind in putting performance pay type of activities in that loop.

So every year we have always had measures or metrics that were related to performance pay. And when you're talking about changing to the culture of cybersecurity years ago -- 10 years ago, I'll be the first to admit cybersecurity to me was getting my antivirus updated on my computer and that was it. Today it really consists of various things, starting, one, with your people. You have to train. You have to make them aware of things. You have to continue to hit those exercises to get them to the right behavior that you want, phishing exercises, for example. Don't just do one phishing exercise a year. Do 10, 15, every how many it takes to get that culture to start looking at those external emails differently and not clicking on links.

Processes, the standards are a big part of that

and our internal controls. Now we know and have knowledge of our inventory. We have controls around protecting those assets. We're concerned about the isolation factor of whether we're using data diodes or physical air gaps, whatever the case may be. We have patching processes. All of these things change the culture to help us look for these malware detections and intrusion detections.

And lastly, is our technology and I think we're now moving into that phase of our process, which is making sure our vendors give us good, high quality technology of our computer systems so that we can bring all this together as one business unit to support our system. So we've been doing it for a while that way. As far as our performance, it was geared towards changing that culture. From the building and workforce perspective or question, that is always a tough one because the electric utility 30 years ago was the place to go to out of college. Today it's harder and harder to pull those college students, so we're always looking for ways that we can help encourage that.

Once we have them in place, the Department of Energy, Department of Homeland Security, Department of Defense, they have very good, knowledgeable people at getting training. The industry can learn from getting training from those organizations as well. I would ask for the Commission consider helping us foster that along even

further than what we've done.

COMMISSIONER HONORABLE: Thank you. And I hope we'll accept that challenge because we do a terrific job, if I might say so, of working with our state colleagues, with industry. If I go out on a tour of a construction site and if I see something that's maybe not quite right -- I'm not an expert, but I might kindly say would you all be open to an architectural review? I might mention it to Joe and to Dave and we've really fostered some great relationships that way. It's not a "gotcha" exercise. It's our way of really helping to strengthen your physical security, your infrastructure, your grid security and so it helps us all.

So I think you're right in that we can always find new opportunities to support the work that you're doing. And we, too, are challenged with that. We happen to rank really high for attracting millennial to our agency and we're proud of that. But then, some of you guys like to pick them off after a few years, so it's an ever-evolving thing for us.

Is there anyone else that has a comment? Yes?

MR. BALL: In our written testimony, we referred to hybrid skill sets in cybersecurity and this may be something that Michael can expand a little bit on as well, but it's easier to find individuals who are familiar with cybersecurity when it comes to traditional IT and

Windows-based infrastructure. The more difficult skill set to find today is individuals who have a power systems background who is familiar with the OT technology and understands what it means to build cybersecurity into the OT network. And for us, inside of AP, that would be our SCADA network.

COMMISSIONER HONORABLE: Commissioner Scott?

COMMISSIONER SCOTT: Again, from the microcosm of New England, I just did some math here. Out of the five major utilities that we've been working with in the past four months there's been four staff changeovers. You know four key people that we were working with say, okay, I'm leaving. And the good news is the utilities are committed to this, so they're able to say, okay, here's the person who's going to replace them. But again, I'm not sure, but my guess is when you have people of these types of skills are very marketable and they're very mobile.

Having said the obvious, and you've worked at a commission at the state level, we can't hope to attract with other people. And I mentioned the Maine experience. That was the stars aligning just right, so you had a gentleman who is not for the money. He wants to relocate to a certain area. He has a retirement, so we're able to capitalize on that, but that's a big challenge for the states. We can't attract and retain the people with those types of skills.

COMMISSIONER HONORABLE: And I appreciate that. And honestly, I'll admit this; I've called people and said enough. You've taken enough of our people after the third swipe. One of them may be sitting in the room today, so I won't say the entity, but I did call and say enough already now. We've got work to do too. Leave us some of our good people. But it is a challenge for us and this isn't a fluff issue for me.

When I came to FERC, 40 percent of the energy sector was eligible for retirement. When you think about this most important function of ensuring it's security and it's safe, and I just said it in a speech a couple of days ago, what's the point of having affordable, diverse energy if it's not safe and secure. And so the work that you're doing and our efforts to attract people to carry it out is key. And I'm preaching to the choir, but I appreciate that you've taking the time to share your experiences. Anyone else?

MR. ASSANTE: I would just add that coming from a training organization it's important to note that power utilities are the leading sector in industrial and infrastructure area training their staff, and the training goes to the place where we've seen automation professionals, power engineers, even dispatchers receiving cybersecurity training in order to understand that in lead teams. So

we've definitely seen that from the electric sector.

I do think the standards and the awareness and the industry's understanding of its importance to reliability has driven that. And I would say that the grid exercises is also an incredible forum which has brought both the engineering disciplines and the IT support and OT ICS/SCADAS support groups together to deal with multi-facet scenarios.

And in my testimony where I called for having to deal with things like operating protocols, one of the things that Ukraine taught me for sure was that the attack was absolutely structured in 2015 against the dispatchers. They lost the UPs and lighting and their phones in their own control centers and it was very clear that understanding that. And I do believe the grid exercise platform has been an incredible to industry and government partnership in order to be able to accomplish some of that learning, understand it, digest it, and develop the protocols that we'll need to deal with these types of things.

COMMISSIONER HONORABLE: I often say there but by the grace of God we go, and so we have the benefit of learning from that and employing it in our operation centers.

MR. SACHS: Let me just make two quick points. One is that this is fortunately not a new problem. I can

recall as early as 1999 when the Defense Department was first wrestling with what do we do about cybersecurity outside of the classified world, that one of the questions brought up immediately was what do we do about SCADA and so the term was in popular use almost 20 years. And we knew that there was growing issue and we knew there was a workforce problem.

This may have been talked about, this Grid-X thing that we do every couple years I think is so unique to us, but we're also seeing in the educational world a growing number of colleges, universities, and even high schools that are doing security-type exercises. And we're seeing this begin to grow almost organically, almost like sports, soccer, baseball, other things, very competitive.

This is good news and it's something we need to leverage and enhance and really kind of make it an all American thing that getting involved in cybersecurity as a career field early is absolutely what we want these young kids to do. Don't wait until you're 30 or 40 to discover cybersecurity, but discover it when you're 13 or 14 and really just dive into it.

COMMISSIONER HONORABLE: All I can say to that is Amen. And I spoke at an event in Houston maybe last year and an eight-year-old asked me about cybersecurity and it blew my away, but I thought kudos to you guys. I mean

someone has been talking about in a way that got the interest of an eight-year-old and that's what we need, so I couldn't agree with you more, and I won't say another word after that.

MR. GOVINDARASU: Just a quick comment, I think these are excellent points. As you know, the cybersecurity for the grid is an interdisciplinary field. We need to educate engineers, our future students who are featured in -- bringing both the cyber and physical flavor. I think a lot of universities have education program in cyber physical security for the grid funded by DOE, National Science Foundation, and so on.

As part of an effort, there are also hack-a-thon, cyber difference competition creating markup similar to the grid exercise. Those things are happening. Those are very well-established efforts. But the critical thing for both things to be successful is industry/university partnership. Universities they do things well with the education, but they need to understand the real, practical scenarios and those partnerships need to be center, but there is a lot more to happen.

That may not only be a training feature engineers, but also the current engineers who are in the field they could take certificate courses or graduate courses or cybersecurity training sessions like grid

security conferences and so on. So the universities have a critical role in workforce development, development in partnership with industry and other Federal Agencies. Thank you.

CHAIRMAN LA FLEUR: Well, thank you Collette. And thank you all very much. I want to especially thank Mr. Wales for coming over from the DHS. It's always important to have our government partners here.

A very interesting conversation, I was just looking behind me because my summer intern this summer, who was here for the morning session, but I think she's writing a speech, won some kind of hacking contest. I don't remember, first place in some Hack Princeton or Hack America or Hack-a-Thon, which I believe is just what you were talking about. You see they didn't have that when I was there since I don't even know what it's called.

I have a couple of questions. The first thing I want to talk about, Marcus, you mentioned in your pre-file testimony that there were new data sources to better understand the security landscape and Mr. Assante talked about -- I believe it was you, Michael, who said that the standards are too backward looking and we need more leading indicators of things.

Are there leading indicators of cybersecurity issues that we can develop? You know you've talked about

faint signals in other places. Some of the standards, I think, are intended to do that, intended to think if you're not careful about passwords you might not be careful about firewalls or air gaps or other things, but are there more cyber leading indicators we can look for in the system that will help?

MR. SACHS: We've certainly learned that cyber is not like a predictable system, so typically, when you do standards it's because you can predict a behavior. In Physics, you know like a railroad.

CHAIRMAN LA FLEUR: Like a safety pyramid, if you do so many of these you'll have so many of those.

MR. SACHS: Right. But security does have a baseline. There are some fundamental things that we all do. We call it hygiene. We call it best practices. That, of course, can be done, but where the adversary works is above that and the adversary doesn't care how compliant you are. Doesn't care which standards you've done. They don't care. They're just looking for ways to get in. So this goes back to then, well, how do find -- what are those faint signals? How can we see where the adversary is punching around looking for a way to get in?

You're familiar with our CRIP Program, the Cyber Risk Information Program? That generates an enormous amount of information about ourselves. We're able to look through

that information and find things -- as I was saying earlier, look for things that aren't normal, something new that's happened, something we can't explain and began to ask lots of questions. Some of the best analysts out there are those who are curiosity seekers. They just see something that doesn't look right and let's just start going down that road to see where it takes us. We may not uncover anything or we may uncover some brand new malware nobody's ever seen before, a new technique.

The information sharing, as Brandon mentioned of the AIS Program, we're embracing that. We're building out a pilot, so we're going to do the automatic information sharing. So again, if some entity sees something that's not right let the computer share that with other computers. The human tends to slow things down, but the human mind is something very special and can see things that are different. It can ask questions that a computer can't ask. A computer often doesn't ask why is something happening. It just says it is happening, but the human mind could say why and connect dots, as we like to say it.

So I think as we are getting better at understanding what security is, we're getting better at detecting when security events are happening and then getting better at analyzing them and asking that "Why" question so we can get the word out, so we can get others

involved. And always I'll go back to the partnerships. The more people that we have -- it doesn't matter who employs you, whether it's private sector or individual or government, it doesn't matter. If you've got a good brain and you want to jump into this, the ocean is wide open and we need people there. We need them collaborating across all these boundaries. It's not competitive. You know this is all about security of our way of life and so the more people we have doing that the better it is for all of us.

CHAIRMAN LA FLEUR: So you need a human to spot the patterns, but can the computer like toss up the data? I remember when we used to have the mainframe and you actually had the code. You're not going to actually be -- like I know you're too young to have had those punch cards that we had, but I mean you're actually looking for the

COMMISSIONER HONORABLE: Yes, I'll admit that.

CHAIRMAN LA FLEUR: But you know nobody has time to look at all the little things, but somehow you have to look at it electronically, right?

MR. SACHS: You could find a card in a fortran deck, yes.

CHAIRMAN LA FLEUR: If you got one wrong, it won't run.

MR. SACHS: It messes up the whole program. It won't work. And then you get to the end of the line and run

it again.

CHAIRMAN LA FLEUR: But there's the equivalent now, even though it's no longer a card where there's some thing in there.

MR. SACHS: Large datasets is the challenge because we're accumulating all this data, terabits of data. The human mind cannot begin to grasp this. This is the challenge that Google and Amazon and others have overcome where they look at very large amounts of data, use the power of computer to go find things and present it to a human in a way that our brains can interpret it. That's something we're also beginning to understand in security is how do bring something out so the human can see it and it's only through your eyes. We can't really taste cyberspace or hear cyberspace. We have to look at it because that's the way our brains work and so the challenge is how do you put something on a screen that a computer can express to an human so a human can understand it and begin starting to ask the questions and then the computer can go back and maybe answer those questions. A lot of work being done in the research community, a lot of work still to be done there, but data visualization is one of the big key items and security visualization is key piece as well.

CHAIRMAN LA FLEUR: It's fascinating. I know Michael is -- has stuff to say.

MR. ASSANTE: Thank you. I would suggest that in deconstructing some past incidents that have affected control systems particularly the signals would not be described as faint, but they would be described as deafening. In fact, some of the incidents would demonstrate that adversaries were experimenting. In fact, we've developed what we believe as models to look at in order to have a physical affect on a system it takes quite a bit of effort on the adversary's part in order to learn and know and have confidence that if they do something they're going to have a desired affect. And in the case of Ukraine, there certainly were observables and we wrote about those significantly with the EISAC about what to look for. And for example, some of the switches that uploaded most of (1:11:07.8) to they typically aren't touched by individuals. Once they're commissioned and tested, they're never managed. And when somebody goes out to touch them, it should be a big indicator that you know why are we doing that, right?

And also, I would say in the area you talked to earlier panels about data analytics and to Marcus's point, I've seen incredible prognostic technology advancement in this industry. In fact, arguably, I've seen individual utilities understand machines to a level of fidelity that is impress to be able to predict failure so they could take

failures on their own terms. I believe we have the technology to apply that for the cybersecurity challenge.

Again, if you go with the basis that, in fact, this new malware that we've discovered it just doesn't work all by itself. You have to get it into position and then you have to have this confidence that you understand exactly how the utility's operating breakers with the protocol, it's AD&P3. There's different ways to do it. And in order to experiment, you want to catch them in their experimentation. Prognostic technology could see the slightest tampering, an unauthorized circuit breaker operation in a small part of substation is something that can be detected. And I do believe that the industry has the capability of going down that road. They need the flexibility to try to conduct that innovation. I've been working with people like General Electric. GE has been looking at that. They understand their machines very well. They're looking at how can they use their models to identify tampering within those same systems. So I believe technology and that data analytic you talked about earlier is a tremendous opportunity for us in order to start outpacing the attackers.

CHAIRMAN LA FLEUR: Thank you. I was going to ask who could we learn from. We just heard Google, Amazon, and GE -- I mean people out there that are doing this.

I think it's related, but you talked about, at least in your written testimony, about Internet signatures, which I guess where you see where something is coming from and Commissioner Scott mentioned the fusion centers like in Topeka that compare one set of data to another set or data or whatever. Do we have the right protocols to share that? Do we need to do things differently so if one company sees something it gets to the EISAC and gets to other places? I mean I don't understand it well enough to know, but it seems like it would be rich area to prevent problems.

MR. SACHS: I'll give you a brief answer and then I'll pass it to the Commissioner, but oftentimes organizations like us or a private sector group or the government will see something and want to pass it to others. We use a process called TLP or Traffic Light Protocols to handle the sharing of information. So when you discover it, you have to be careful about it. You don't want to just broadcast it to world because your adversaries may see, but you wanted to give it to a trusted partner who can do something with it, so you'll call it TLP green or amber or whatever.

On the government side, oftentimes, it's detected in classified channels and so it's got a classification wrapper on it and we have to get that wrapper off, get it down to unclassified. There's a delay there.

When the machines want to talk to each other, they don't understand any of that. That's a human hindrance and they love just chitchatting back and forth, but it takes a human to connect two computers together and often the humans are bound by legal barriers, bound by information and trading barriers, bound by fear that the adversaries might get in the middle and watch the machines talk.

So there's a lot of good technical things we can do, but there's a lot we need to do in terms of the human understanding of why we need to rapidly share and barriers that are artificial, largely legal, cultural, that we need to take off the table.

I know we often have good stuff we could share with others. Others have good stuff that they can share with us, but many times it's the people that get in the way, not the technology. That's not stopping us. It's the process. The Commissioner may have the same sort of observations.

CHAIRMAN LA FLEUR: Bob, I know you talked about fusion centers in your testimony. I know what some of what they do is confidential, but I guess are there ways we can share this data better?

COMMISSIONER HONORABLE: I think it's a great question because I think with some of the fusion centers that is the challenge, that if you don't have a clearance

you really can't really participate.

COMMISSIONER SCOTT: Well, that is something, as you're aware, New England is exploring. We have a fair working relationship with the Kansas Intelligence Fusion Center. We're exploring that type of activity, but Commissioner Honorable is exactly right. Obviously, that only works to the extent that the utilities involved have the appropriate clearances for obvious reasons.

So it brings in a world of other issues like spillage and mitigation strategies, but I will say at least in New England, and I think Marcus mentioned DOE CRIPs, not all of them, but most of the utilities we're working with on that type of activity are also using CRIP, so it's not one or the other. They're finding extra value having gone out to Kansas and worked a little bit with them. It's an exclusive club, if you will

CHAIRMAN LA FLEUR: In your perfect world, anyone, I mean how many people within a utility would have a clearance. I mean I got to a lot of briefings with CEOs. I mean I was the CEO. I didn't do the computers, right? I mean I was never a CIO. You'd be insane to make me one, so I mean you'd brief these people who might have clearances and I mean so how -- if we had a perfect system where the right people had the clearances, how deep would it have to go.

COMMISSIONER SCOTT: There's multiple questions there. What level of clearance depends on how deep you're going to go also. Generally speaking, in my view, at least to get started obviously there needs to be CEO buy-in. The CIOs ideally would be involved and then you have the actual people doing the work, right? So that I would argue for two or more, I think, depending on what you're doing and why you need that. And I say buy-in is as if there's a mitigation strategy that's developed based on that type of data that costs some money, obviously. Now that has to be sold up the chain for obvious reasons and I'm a regulator at the moment, so certainly get that.

That requires the buy-in, so at least to start I think you need more and my guess if the utilities were to go down this path that once there's a faith in the system, if you will, that perhaps could get lessened. So I'm not suggesting that clearances are easy. In a post-normal world, if I were on the federal side I would be wondering too how many of these do we want to give out, et cetera. It's a challenge.

CHAIRMAN LA FLEUR: And I wasn't arguing that CEOs shouldn't have clearances. It's just they're not going to operationalize it into the machines, I assume, unless they're very unusual.

MR. WALES: Let me try to provide a little

context to this, both the value and the potential overestimation of value in providing security clearances. I think we've used security clearances that we provide to the private sector and DHS itself has cleared somewhere around 1500 to 2,000 private sector owners and operators throughout the country.

They provide two purposes. One, is they're helping us, so when we have classified information we can share it with them and they can provide context from how the industry would view this information. Are there things because of their unique expertise and understanding and the kind of activities that they oversee that they could read into this intelligence that government analysts won't be able to do.

Second, it helps to provide broader environmental understanding of the nature of the threat. It is not going to help with network defense immediately. That's why we spend a lot of time trying to figure out how to get the kind of information that's going to make a difference to network defenders down to a classification level that can be share because when we bring 20 people into a room and provide them with a classified briefing they can't just go back to their office and tell their network defender put in the following classified hash into your firewall. You know it doesn't work that way and so

clearances are an important part of what we do in terms of the information sharing. We think it helps make sure that we are on a common baseline with the leadership inside of organizations and with the key people who have to monitor their networks, but it is not going to be a panacea for even emerging threats and risks.

It's not going to stop necessarily the next Ukraine if we have indicates of the kind of activity or the kind infrastructure that that cyber operator was using to target those networks. So we think it's important, but it is, by far, not going to be enough.

CHAIRMAN LA FLEUR: So I'm going to translate back what you said. It's not just getting some people clearances. It's getting the data to a level that it can be operationalized. Okay.

MR. MITCHELL: If I could just add a little to that, we always are pushing for the information to become actionable. You know get it out to the industry. It doesn't have to be classified. It's just utilizing classified information to inform an actionable alert that would come out through the EISAC or some other form. And then we, as the industry, would utilize our trusted networks of saying trust us. We're getting this information. We need to act on it. We need to move on something and it is of highest of importance.

Unfortunately, and Commissioner Scott brought up the issue with Burlington. That was followed. Everything was done right by Burlington and then they went through the mud in the media. We lost trust in the system with that, but we are rebuilding that through these efforts and we encourage that trust rebuilding.

CHAIRMAN LA FLEUR: I want to ask one more question that's on a different cybersecurity topic. One thing you hear a tremendous about is the increased cybersecurity threat from all the distributed resources and the Internet of things. Frequently, that is said by people who might have other reasons to not like distributed resources, so it's hard, as always, to unscramble this.

I generally feel like if we're doing our job in this building, then if something comes in from a distributed resource and it gets up to the Bulk Electric System it shouldn't be able to go across and be a cascading outage because we've stopped it at that level. But I have all these experts here. How much of an issue is this, the fact that we're going to have a lot more distributed resources and is there something we should be doing about it because it's very (1:22:24.6)(in the land? You hear it as sort of a throw away line in speeches. And by the way this going to become much worse because of blah, blah, blah, blah. Interested in your thoughts.

MR. SACHS: Just briefly, it's not the distributed energy piece. That's electricity physics that we worry about. From a pure security perspective, it's introducing a new device that you don't know about. It has possibly a connection to the open Internet that we don't know about and there are billions of people on the Internet that we don't know about.

In an earlier world, it's all protected. These things that connect together and produce and deliver electricity are private. When you bring in an Internet of things or anything that's connected, it doesn't matter what it's doing, if it's connected you're now extending what we call the attack surface. That is the fundamental issue. It's not the physics of it. It's not the politics of it. It's the fact that you're connecting the public Internet, possibly at the bottom, which could then open a door to come up through the bottom of the network through distribution and perhaps do damage.

CHAIRMAN LA FLEUR: So in the olden days, which wasn't very long ago, the meter on my house only the electric company could read it. It had a lock. I never touched it. It was just all there. But now if I have my phone and I can turn things on and off, then a lot of data is somehow around; is that sort of what you're saying?

MR. SACHS: It's again not so much the data. If

the meter can be reached anonymously by somebody we don't know about on the Internet, there could be a problem. If the meter can only be touched to authenticate it; in other words, the electric power company is the only one that can read it and talk to it, we're fine. There's no issue there. It's that unauthenticated piece that's the problem.

CHAIRMAN LA FLEUR: So is this a problem for the Bob Scotts of the world or is there something FERC should do?

MR. SACHS: No.

CHAIRMAN LA FLEUR: So it's at the distribution level, but it somehow -- Michael's going to help us.

MR. ASSANTE: I was going to suggest two dimensions. What we really need to watch out is the concentration. And when I say by concentration, it is the access and we like to do this. In a market-driven economy, we achieve efficiency and often in the achieving of that efficiency we build architectures were we actually concentrate to be able to touch lots of these things.

In fact, I've been amazed sometimes about seeing distributed resources throughout the country that's actually in a maintenance sense monitored at a single location. Now the question in my mind in these architectures is when we do interact with these devices in a distributive fashion when we're interacting how many should be interacting with it at

any one time? Most business cases means we're going to deal with one, two, three, or four machines to tune or make a change or adjustment, but the architectures allow for touching all of them. And these are the types of things from an engineering perspective we need to take note and so it does extend into the distribution systems. It does extend into renewables, for example. But again, I believe it's about secure architectures. There's lots of benefits for doing it this way. We should absolutely be moving forward in that direction, but we need to bring that security requirement into the engineering design of those systems.

MR. WALES: Let me just give you two ways of thinking about this. On the one hand, the distributive resources within a particular utility if those are protected the same way that they've protected the rest of their operating systems, meaning that there's not Internet addressable systems. You can't get to them from the outside. You can only get to them from inside of the network, then they're as well protected or not as well protected as the rest of the operating systems that they have on their grid.

If, however, those are Internet addressable, which means anyone in the world can immediately find that and begin to look for weaknesses, the adversary has a lot of

time and they will eventually find weaknesses in those systems. And if, depending on how the configurations work, if they get in they can move elsewhere and do a lot of damage. But I would say that's a little bit distinct from, I think, some of what you're hearing, which is kind of the second issue, which is just the large number of Internet of things potentially provides an adversary a lot of toys to connect with and then use those an amplifying attack on other infrastructure, which what we saw with the DDOS attack using the Mirai botnet both net late last year where they just created a huge, loud service attack because they were able to get contact with all of these Internet addressable Internet of things devices -- you know little things in your house that you don't even think about, but they're connected to your Wi-Fi. They're Internet addressable and an adversary can eventually get contact with those.

So in terms of where FERC is and where I think NERC is the question is how do these standards cover widely dispersed devices on a utility's operating network? What are the requirements for security around those devices? And if they're just part of their regular operating system, they are just now sitting at your home as opposed to inside of a substation they can be well protected.

CHAIRMAN LA FLEUR: But technically, jurisdictionally we're doing the Bulk Power System, so if

they're on the distribution side of the meter, unless they're going to come in, jurisdictionally, at least, the states would make the rules.

MR. SACHS: Only if you're talking about a grid device or distribution device, but what Brandon's talking about is much, much bigger. Could it be FCC? Could it be Consumer Product Administration? I mean there's a whole lot of other animals here that have to be brought in. It's not just a NERC/FERC versus states to have a discussion.

MR. BALL: So the key component of that from a utility perspective is the architecture of that infrastructure. You have to have the ability to separate your corporate network that has access to the Internet from your operational network or SCADA network. And that is probably the key to maintaining cybersecurity on anything that can be or could be controlled from outside of the utilities.

CHAIRMAN LA FLEUR: You didn't necessarily make me feel this wasn't a problem, but at least you made me feel like you understand it very well and that's a very good start.

MR. GOVINDARASU: I think that IOT is the new thing that anyway that comes small on the consumer side, but coming back to the bulk process that will sell. The smart grid technologies, like whether you call it smart sensors

like PMUs, like communications technologies, distributor controllers, all kinds of things they do increase attack surface, because those are IP-enabled devices. They are connected somewhere. You have more access points.

The question is whether those access points are available to adversity or someone outside. How do you protect that? So assessing that attack surface and also minimizing that attack surface of risks. I think those are important. It is not to say, oh, we should not automate, then we are going backward. While we are automating things, we need to make sure that a security is in place. There's secure architecture isolation, what kind of access control has to be in place or authentication and so on. I think it has to be carefully planned. That is where the standards come into place. A weak systems are allowable to be accessed outside. Some other things should not be allowed, then it should be within the parameter and things like that. I think it has some flavor of those things. But as we talk about IOT and other things, one has to be very careful about defining those standards and what those qualities are.

CHAIRMAN LA FLEUR: Well, thank you for that clarification because some of those smart grids are very much on the Bulk Power System. We're talking PMUs on big transformers and things. Thank you.

MR. BARDEE: So I just have a couple of quick

questions, recognizing that we are getting near the end of our day.

Mr. Assante, in your written testimony and again in your oral remarks, you reference an effort by INL involving consequence-driven cyber-informed engineering and you said that it's a way to engineer out the worst cyber risks from our critical energy infrastructure. Could you talk a little bit more specifically about that?

MR. ASSANTE: Sure. And this goes back to, I think, a question of an earlier panel, this idea of fallbacks or analog, but really the bigger concept is taking the strength of industry, which are the deep expertise and trying to understand what type of consequences a cyber attack can enable within the power systems or assets in which the utility controls. By taking that additional prioritization, this idea that consequence first, let's look at what would be something would be more difficult to recover from. I mean that allows them to really identify and understand at a very deep level how do these systems work and how have they been engineered as we've deployed them and then reconsider some engineering choices and tradeoffs.

Ideas like simply removing a soft cyber control and actually having a dry contact might be a very cheap engineering solution that removes an entire risk of a

machine being damaged irreparably. So the idea is to get that level of depth. It forces utilities to break through assumptions, thinking that we're done this way and that way and we find that there's a lot of false assumptions when you actually go look how systems are put together and what is possible. But also, again, it builds on the engineering strength of utilities.

And the reason why I believe it's absolutely necessary is adversaries today are demonstrating the capability that we must, as defenders, go beyond cyber. I appreciate that some of folks here believe in separate is absolutely important in terms of separating your business systems from your control systems; however, the adversaries that we've watched are getting good. They understand that separation will be there. They're developing delivery techniques to beat that separation. Two factor VPMs have been defeated by certain actors around the world. So some of these controls that we rely upon are no longer as effective as we believe they are and so going beyond that to understand, I think, what is our strength in applying engineering to this problem has lots of benefit.

And again, when we talk about focusing on large outages and losing big parts of the system that's where a constant-driven approach really brings you very quickly. You begin to understand that it might an aggregation of how

we're interacting with several low or medium CIPs assets as defined by the standards because the way we've architected our interaction this is an area that we need to go back and readdress how we're engineering. It will inform cyber defense efforts too. Having a deep level of understanding goes back to your cyber defense strategies.

It allows you to identify jump points where adversaries need to get to in order to be able to affect some of these things. And I would also argue as my last point the malware that we've seen the way it attacked the system to cause disruptions is absolute a normal way should that the system should communicate. It's using the industrial protocol that we have implemented to open a circuit breaker.

There are some features within the malware, like an exploit against protective relay, which would have a signature that looks like it is something that is non-normal, but everything else looked absolutely normal. So I would encourage utilities get a deeper visibility into how systems communicate and that begins with an engineering understanding, which I know the utilities have and possess that capability.

So working with our partners, we believe that's going to provide the biggest reduction of risks because the type of risk we're most worried about come from your

significant risk-type of dimensions. It's not from the 12-year-old hacker or the 14-year-old hacker, if you will.

MR. BARDEE: So to me, it sounds a little bit like an idea I've heard about in the context of our physical security standard, CIP14, where utilities will look at their system and say, well, for now we're going to protect the ones that are critical, but in the future we're going to build out our system in a way where we don't have critical substations. We're going to reduce our risk by redesigning going forward.

MR. ASSANTE: That's absolutely right. The long-term learning as to what enables a terrible consequence through cyber means what could happened informs design decisions in the future and so we're starting to see some of that activity as we're engaging in some of these methods with industry and industry partners. So I believe that's absolutely right and bringing in the suppliers to partner on how they are architect to design their solutions is a vital aspect to this as well, so this really an opportunity for shared learning and the ability to be able to move that learning. And I believe a lot of what I've seen in deconstructing real-world events would indicate that that type of thinking is important.

I'll give you one last example in a nuclear context and I'm very proud to see the United Kingdom is

adopting this. We've moved to digital safety systems for our advanced light water reactors. That's a move away from analogs. You had to. But the question is not an analog device, but the question is should we be using general purpose controllers in technology for that safety system or should we have a fallback system that is a highly deterministic and very difficult or I would say limited programmable device that is performing that final safety function to avoid what could be a consequence that's not tolerable.

Those types of engineering efforts need to be understood by the suppliers. Economics will drive us one way, general purpose. Knowing where the limits are and where the thin line, if you will, would be for consequences that we cannot tolerate would require us potentially to go the other direction.

MR. BARDEE: And one last topic I wanted to raise with Mr. Sachs on the reporting requirements for cyber security the State Reliability Report notes that we had no reportable incidents 2016 and even in 2015 and I understood from the report itself, and I think your remarks or maybe Mr. Cauley's earlier in the day, that you all are taking another look at are there other metrics we should be looking at. Could you describe that a little bit?

MR. SACHS: Yes, thank you, Mike.

So this kind of goes a little bit to what Mike's talking about is what's the consequence you want to avoid and we want to avoid loss of load, so we go and look and see has there been any loss of load caused by cyber and the answer is no, or by other security events. And so you report that and say all is well, but it kind of gives a false impression.

Yes, the consequence has been avoided, but it doesn't mean there's not a problem or that there could be a problem or something hidden and that's our challenge, guys. How do we go look for those types of things we can see, measure, have reported to us, and begin to do that analysis that even though there's not been a lights out or loss of load or the consequences we don't want to happen that we still become cognizant of what else is going on and so we can get that early indication.

Currently, as you know, we've got mandatory reporting at certain thresholds and that's working fine. Then we have voluntary reporting beyond that, a lot of improvement we can do there, but also we have to recognize we have seen a lot of improvement in the last few years. The amount of voluntary reporting is definitely on the increase and we want more of it. But like anything else, there's that fine line of do you want to move out mandatory piece so people feel compelled to report, which means

they'll only report what they have to report or do you incentivize the voluntary side so people would feel more comfortable with voluntary sharing. They'd feel if I put something in I'll get something back out. We feel that's the proper way to go. What is that incentive? Don't know. That's part of what we need to work on this year and the coming years is what can we do to help increase that voluntary sharing.

Can we use the fact that the machines automatically record everything they see? You know the logging functions that are built into virtually everything. Can we get that because that's not an opinion? It's not a survey. It's facts that the machine is recording. Can we get those logs shared? Can we get telemetry off of CRIS and CAS and some of these other new programs? Can we study that telemetry and look for those faint signals that you hear us talking about?

These, I think, are areas rich for the next coming years of exploration, things we can do that don't require more mandatory sharing, but can look at what we're already sharing and see what we can pull out of that and then encourage more of that voluntary, particularly machine-to-machine type of sharing of knowledge.

MR. BARDEE: Then last question, again related to the reporting requirements. Whatever the reporting

requirement is or whether there's voluntary reporting or whether there's voluntary reporting on top of that that's much more rich right now the NERC Report puts out just a number and the last two years it's been zero, but in prior years there's at least been a couple of events, I think. Is it possible for the EISAC to take the information it has, whether it's mandatory or voluntary or it makes a difference which one, and provide at least some additional information about the nature of the event that have been reported. It would have to be at some fuzzy level of granularity and certainly anonymized, but ISC CER, for example, puts out an annual report that says, you know, in this sector we had "x" number of events last year. Is that something the EISAC could do?

MR. SACHS: I think absolutely that's something we can do. In fact, in this year's grid resiliency report the chapter on grid security is different from what we've done in the previous two years where we actually did look at 2016 what was reported to the EISAC and tried to tease out what can we learn about what was reported.

Granted, in 2016, we're still ramping up. In '17, we've already surpassed the entire year of '16. We've already accumulated in '17, which is good. So next year the report will be that much richer, but what you're hitting on is exactly the direction we need to go in. The EISAC pulls

in a lot of information. We analyze a lot of stuff; put a lot of reports out. We can also analyze what we've analyzed and create a much better picture, at least orally describing what we're seeing and what we're learning. What's going on beyond just what the machines are talking about, you're absolutely on the track that we're on.

MR. ADREJCAK: Just a couple of comments and then one general question, I guess. Greg, you'd mentioned earlier about phishing attempts. There was a report that came out today about a quarter of the Australian utilities were just hit with phishing attempts, so it's not something that's easily going away. I mean it's obviously still out there, so it's very on point.

Second thought, Marcus, you talked about getting these folks at a young age involved in cyber defenses. I was recently at a military exercise last week where we had all branches of the Military, along with a lot of friendly nations there, nice big scale drill exercise. They genuinely were excited about it, but what I found out was nobody wanted to be the defender. They all wanted to be the attacker and that seems to be the biggest problem I think we have right now is folks don't want to be the defender. It's more fun to be the attacker.

MR. ASSANTE: In fact, you know an assistant administrator is the defender. You talk to somebody who's

in 10th or 11th grade and you say do you want to be a cyber attacker or do you want to be a system administrator? You know what's the response? But much like in the Military, we teach young servicemen and women how to defend at the same time we teach them how to attack and you learn that your weapon, whatever your weapon system is, is both for defense and offense.

When we teach people how to be system administrators, we often shackle them and this is a big problem in the Military. You know thou shalt not do anything other than these things and if somebody bad comes in call this other group. You are not allowed to go elsewhere. So what do the kids want to do, they want to go work in that other group because they're the ones having fun because we shackle the defenders.

So that's part of this mindset we also have to think about and it goes to what many of us have been saying here. There's new rules we need to come up with, new approaches, new ways to thinking about not just for the kids, but even how we operate in this cybersecurity world that's very different from what we've been doing historically, which is more of a safety-oriented type of world and very predictable. This is not as predictable.

MR. ANDREJCAK: Mike, I guess my final comment is directly more or less towards Mike and I guess

Commissioner Scott you as well because you kind of tied this issue together, but I read a really great article that had both you and Robert Lee from Dragos in Wired Magazine that came out very recently, which really shows both yours and his dedication. This is not just a job, but it's obviously something we all live. This isn't like a 9:00 to 5:00 thing. When it happens don't call me at 8:00 o'clock at night. You guys dropped what you were doing to go address a big problem in the Ukraine and I guess I was concerned about what are your thoughts about getting the information out there quickly versus getting the information right, as Commissioner Scott had to deal with, with the Vermont issue?

MR. ASSANTE: It's a critical question, difficult. As you can imagine, when any events occurs there's a fog of war, if you will, as to what really did occur and getting the right people to take a look at that information.

First, I want to commend the Ukrainians for giving an unbelievable look to the United States Government as to what did occur and that's important. This idea of commitment to shared learning with folks is very important. I think by working in different capacities with FERC and NERC and the utilities industries and stuff, I think this is an industry committed to learning. I think there are massive improvements that we could do in deconstructing

incidents and being able to do that. That type of work needs to be done and it needs to be prioritized.

The tradeoff between quick there's ways to do this. There is what we say tippers out to the injury that says we're not completely sure about this, but these are potential indicators. Here's what you could do with it, but being careful as to say what you can do with it our should be doing with it is where I think we got in trouble a little bit some earlier events that occurred. And in the government holds the role of being -- and so does NERC -- of responsible risk indicator, meaning they are going to get to the real story at some level of very real detail and I think we worked through the stresses of that in terms of communicating about the first Ukraine event. It did take a long time and I think there were no immediate attacks that occurred, so maybe that was okay that it took that time, but in this space we won't have that luxury potentially in the future.

I really worry about a campaign of attacks and I think if we start to experience that we will be forced to very quickly learn as much as we can and get information out as we're going in order so that other utilities can defend themselves.

MS. POINTER: I just had a comment and then a question. The earlier discussion about -- I think, Mr.

Sachs, you mentioned about telling those 13- and 14-year-olds to go out there and do stuff, I'm having the opposite conversation with my 12-year-old. So hopefully, I can convince him to be the administrator or the defender that you're talking about, but right now we're having some pretty -- I won't say difficult, but several discussions about what to do and what he shouldn't do.

My question is actually to Mr. Assante. I think Mike raised the question about engineering and I think you'd mentioned loads and I guess while you're here just what are your thoughts about the reporting requirement for low-impact assets? I know Mike mentioned about -- well, I think actually the conversation was more so on the medium and hot, but you'd mentioned loads, I was just wanted to hear what your thoughts are about loads.

MR. ASSANTE: Thank you. I am concerned that -- and I think that the standards have evolved in a wonderful way in terms of bringing more systems into scope, looking at systems and impact reliability and that's been very important. Some of the things we're learning in terms of real-world incidents could indicate attackers might be trying to operate against multiple utilities or a single utility in scale, which means now that something that we'd look at individually as an assets, as a low asset, but taken in an aggregate of being able to open circuit breakers at

multiple locations you know the impact is as bad as if you would've been attacking larger substations, 500kv and larger.

And that's a concern. It's obviously more difficult. What we should do is to think about how to architect our system to be able to allow an adversary to achieve that scale. Some things would require them lots of time and it would be difficult to do. Other types of architectures and ways we interact with technology make it easier.

I think if we take a good, hard look at that we might be able to accommodate both, the idea of assets and resources that individually when misused could cause big problems on the system. This mounds or malware that we're talking about has the ability to operate circuit breakers if you could deliver into place were it could communicate to enough substations.

And again, this is not easy, but if you could do that the scale problem comes in and so the load requirements in the standards today, as you know, wrap basic protections, not necessarily the type of protections. We talked about using VPNs. Well, those apply to certain assets, not others and so I think it forces us to go back and look at how we're interacting with a larger deployment of technology.

MS. POINTER: Thank you. That's all I have.

CHAIRMAN LA FLEUR: I just wanted to first start by thanking all of the panelists for your very thoughtful comments. I think it's been an excellent day. I think some views were rich, a very rich discussion. And thank all of the organizations you represent all day long for keeping the lights on, small detail, that's what this is all about. So thank you for what you do.

I want to thank the people on FERC staff for all the work in setting this up, especially Mike for chairing it, Lode White for doing a lot of the work to organize it, Sarah and others, everyone who pulled it together.

And finally, I just want to thank my partner in crime here, Collette. When we sat in this room last month, I said I hope this won't be the last time we sit in this room together.

COMMISSIONER HONORABLE: And it wasn't.

CHAIRMAN LA FLEUR: And I equally hope that today, but I'm less sanguine that there'll be a lot of other times.

COMMISSIONER HONORABLE: Cheryl, I feel like the runaway bride. I don't know if I'm coming or going.

CHAIRMAN LA FLEUR: I think you brought so much to this discussion and to the Commission, particularly with your relentless focus on customers and also your constant reminders of what we need to do with our state colleagues.

You know one of my favorite songs in Wicked is like -- I've heard it said that people come into your life for a reason bringing something you must learn and I really believe that. And you've also done a wonderful job representing the Commission, whether it's in Brazil or in the singing in the FERC chorus or all the other places you, so thank you for that. I will really miss having you.

COMMISSIONER HONORABLE: Thank you so much.

CHAIRMAN LA FLEUR: Not here, up there.

COMMISSIONER HONORABLE: Thank you so much.

Let me say to Mike Bardee, who continues to lead so well, I was mentioning to someone on the elevator I really don't think our jobs are the most important. Yours are because you hold this place up and you have the institutional knowledge and experience -- when I say "you," all of you and your colleagues and you have been committed to this job. And Mike Bardee went away. He went on a detail very far away. He went to Europe. And when he left, I said the only way I'm going to support this is if you come back, so he has. So thank you.

And I want to thank all of you, and especially those of you who are sitting in the softer chairs. You get a gold star because you didn't get to say a darn thing, but yet, you're still paying attention. Because this work is so important and we know today that challenges are greater than

they have ever been. And I remember when I began as a state regulator 10 years ago hearing that from someone "This job is more challenging than it's every been." Well, it is also and in 10 years it will continue to be, but I know -- and after this long day of our work together, maybe the second longest day of the year, that we are well prepared to be able to continue to work on the challenges that lie ahead.

It doesn't mean we have it all figured out, but it means that we have number of men and women across many sectors, yes, including our colleges and universities, who are committed to helping us solve very challenging issues and that really gives me hope and heart about the work that we can do together.

And let me say, too, to our FERC staff here thank you for supporting this effort that we carry out, not only every year, but each and every day the ways in which you keep electric reliability front of mind for us and I want to thank my staff as well. And to our fearless leader, who has been our chairman, so Cheryl was our chairman when I started here at the Commission and I, in fact, met Cheryl as soon as she became a Commissioner at a NARUC meeting and there were like a million people all over the place, like touching her, is she real? Is that the new commissioner?

And so from the moment that we met, Cheryl,

you've been so gracious. And even when I transitioned here, I joked that Cheryl's advisors at the time were my advisors because they helped me stand up my team and even though we haven't agreed on every single thing, we have agreed on most and it's been an honor to work along side you, along with our other colleagues who've come and gone.

And it's been an honor to work with you at all of the capacities that you've held here as chairman, as commissioner, as interim chair and hopefully, as commissioner and I'll be riding off into the sunset for the next journey. But this has been the highest honor of my professional career and it's so much so because of the men and women I've done it with, so thank you so much.

MR. BARDEE: So that will end the day. I thank all the panelists for their help today and other times when we've called on them and look forward to continuing to working on this mission with you.

(Whereupon, the meeting concluded at 5:10 p.m.)

CERTIFICATE OF OFFICIAL REPORTER

This is to certify that the attached proceeding before the FEDERAL ENERGY REGULATORY COMMISSION in the Matter of:

Name of Proceeding: Reliability Technical Conference

Docket No.: AD17-8-000

Place: Washington, DC

Date: Thursday, June 22, 2017

were held as herein appears, and that this is the original transcript thereof for the file of the Federal Energy Regulatory Commission, and is a full correct transcription of the proceedings.

Gaynell Catherine

Official Reporter

BEFORE THE

FEDRAL ENERGY REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - - x

In the Matter of: :

RELIABILITY TECHNICAL : AD17-8-000

CONFERENCE :

- - - - - - - - - - - - - - - - - - x

Room 2C

Federal Energy

Regulatory Commission

888 First Street, NE

Washington, D.C. 20426

Thursday, June 22, 2017

The technical conference in the above-entitled matter was convened at 9:30 a.m., pursuant to Commission notice, when were present:

FERC COMMISSIONERS:

ACTING CHAIRMAN CHERYL A. LA FLEUR

COMMISSIONER COLETTE D. HONORABLE

FERC STAFF:

MICHAEL BARDEE, (Presiding)

ARNIE QUINN

JIGNASA GADANI

ROGER MORIE

LARRY PARKINSON

LEE ANN WATSON

JOSEPH MCCLELLAND

DAVID ORTIZ

MATTHEW VLISSIDES

MARTIN KIRKWOOD

JONATHAN FIRST

JAMIE SIMLER

ANNA COCHRANE

NANO SIERRA

CYNTHIA POINTER

MARK HEGERLE

LODIE WHITE

ROBERT CLARK

PANEL I: OVERVIEW ON THE STATE OF RELIABILITY

GERRY CAULEY, President and Chief Executive Officer, North American Electric Reliability Corporation

PATRICIA HOFFMAN, Principal Deputy Assistant Secretary and Acting Assistant Secretary, Office of Electricity Delivery & Energy Reliability, U.S Department of Energy

CHAIRMAN ASIM HAQUE, of the Public utilities Commission of Ohio representing NARUC

CHARLES KING, Vice President and Chief Information Officer, Kansas City Power & Light Company on behalf of EEI

STEVEN WRIGHT, General Manager, Chelan Public Utility District on behalf of Large Public Power Council

BABAK ENAYATI, Lead R&D Engineer, National Grid on behalf of IEEE

JOHN TWITTY, Executive Director, Transmission Access Policy Study Group

JOHN HUGHES, President and Chief Executive Officer, Electricity Consumers Resource Council

PANEL II: INTERNATIONAL PERSPECTIVES

BRIAN HEWSON, Vice President, Consumer Protection & Industry Performance, Ontario Energy Board

COMMISSIONER MARCELINO MADRIGAL, Mexican Energy Regulatory Commission

KLAUS DIETER BORCHARDT, Director for the EU Internal Energy Market, Directorate-General for Energy, European Commission

PANEL III: THE POTENTIAL FOR LONG-TERM AND LARGE-SCALE DISRUPTIONS TO THE BULK-POWER SYSTEM

MARK LAUBY, Senior Vice President and Chief Reliability Officer, North American Electric Reliability Corporation

DEDE SUBAKTI, Director, Operations Engineering Services, California Independent System Operator

MICHAEL KELLY RIVERA, Los Alamos National Laboratory

DR. GEORGE H. BAKER, Senior Advisor, Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack

RANDY HORTON, Senior Program Manager, Electric Power Research Institute

THOMAS POPIK, Chairman and President, Foundation for Resilient Societies

SYLVAIN CLERMONT, Director, Reliability Standards and Regulatory Compliance, Hydro-Quebec TransEnergie

PANEL IV: GRID SECURITY

MARCUS SACHS, Senior Vice President and Chief Security Officer, North American Electric Reliability Corporation

MANIMARAN GOVINDARASU, Professor of Computer Engineering, Iowa State University

MICHAEL ASSANTE, Director Critical Infrastructure and Curriculum Lead for ICS/SCADA, SANS Institute

GREG FORD, President and Chief Executive Officer, Georgia system Operations Corporation

DAVID BALL, Director, AEP Transmission Dispatching, American Electric Power

NATHAN MITCHELL, Senior Director, Electric Reliability Standards & Security, American Public Power Association

COMMISSIONER ROBERT (Bob) SCOTT, New Hampshire Public Utilities Commission

BRANDON WALES, Director, Office of Cyber and Infrastructure Analysis, U.S. Department of Homeland Security

P R O C E E D I N G S

(9:30 a.m.)

MR. BARDEE: Good morning everyone. I'd like to thank everyone who's here today and listening outside of the building, and especially thank our panelists, both on this panel and later in the day, for being here and submitting the testimony they've already sent us and for the remarks they'll make today and being available to answer our questions.

Just as a little bit of background, about a little more than 10 years ago Congress approved Section 215 of the Federal Power Act and gave the Commission the authority to approve and enforce mandatory standards for reliability of the Bulk Power System. And since then, we have worked with NERC in this process of adopting and then enforcing the standards.

NERC, through it's regional entities, has really taken the ore on all of that and it's been a good working relationship and I think at this point it's fair to say we have good set of standards. With that, though, there remains work to do. During today's conference, we're going to touch on three areas to explore how we're doing on the reliability of the Bulk Power System and whether there are areas where we need to pay more attention or do more work.

The first panel is going to start with an

overall assessment of the state of reliability, the major issues that we're facing right now. The second and third are going to address emerging issues, both internationally and then in the United States, and the last panel will be on cybersecurity of the grid.

Let me go over just a few housekeeping matters. First, there's no food or drink allowed in the Commission meeting room here, except for bottled water. We would also ask you to turn off your cell phones. We do have a way for people to use Wi-Fi here. There's a piece of paper out on the table outside with the instructions for how to use Wi-Fi, just like that. It says "Guest Wireless Network Rules of Behavior." So if you want to get that a little later and follow that, you'll be able to use the Wi-Fi here.

I would add, though, that if you're using your devices on Wi-Fi, you're not paying attention to us.

(Laughter)

MR. BARDEE: So recognizing that we are a little time constrained, we are going to ask the panelists to limit their oral remarks, generally, to four minutes. There's a clock down here to help you with that. There are a few exceptions because Mr. Cauley is going to be doing the presentation on the overall state of reliability based on NERC's report. We've allowed him a little more time, as we will for our international speakers on the next panel.

Let me just read a statement that is now part of our opening at all the Commission meetings here in the Commission Meeting Room. Members of the public are invited to observe, which includes attending, listening and taking notes, but does not include participating in the conference or addressing the Commission. We will not have a general Q&A with the audience during the conference; however, members of the audience and others may submit written comments in Docket Number AD-17-8.

Actions that purposely interfere or attempt to interfere with the commencement or conducting of the conference or inhibit the audience's ability to observe or listen to the discussions, including attempts by audience members to address the Commission while the meeting is in progress are not permitted. Any person engaging in such behavior will be asked to leave the building. Anyone who refuses to leave voluntarily will be escorted from the building.

So with that, let me turn, first, to Acting Chairman LaFleur for any remarks she may have.

CHAIRMAN LA FLEUR: Thank you very much, Mike, and good morning everyone, very happy to have you here. We have a great lineup of panelists and I've read great pre-filed testimony and happy to have everyone in the audience. It's not only exciting to have people in the

Commission Meeting Room, but is even under normal circumstances, I think, one of my favorite days of the year because it's such a great discussion.

I enjoyed reading the pre-filed testimony and the state of the reliability report. Thank you, Gerry. I just wanted to outline three macro topics, three things that I hope to get from the day as we think about these topics and think about where we're going reliability for FERC 2.0 that will be joining us soon and we'll be moving to the other side of the table again.

First, is where we are in the standards process? As Mike said, we're 11 years into Section 215 and the ERO Enterprise, so where are we? Have we reached steady state? Are we in steady state? Are there emerging issues that we need to focus on and really build up the standards? These are not mutually exclusive, but it might be complementary, or are there ways in which we need to streamline or reduce the standards.

I saw some testimony from some people about selective enforcement based on whether the standards posed a risk to bulk system reliability. Well, all of the standards are supposed to be need for reliability. So if there are standards are not needed for reliability, where are we on the standards? I'd like to get a sense of where we are and where we should be going in a macro sense in the body of

standards.

Secondly, I want to think a little bit about priorities going forward. I always say given the rather unique structure that Congress gave us between NERC and FERC, the success of our reliability effort really depends on our having shared priorities. So as we address emerging issues, be they related to grid security or transformation of the resources on the grid, what should NERC and FERC 2.0 be working on in the coming year between now and when we have our next conference?

And as we look at those issues, what tools should we be using because standards is a tool, but we have assessment and the data work and all of the analysis that NERC and the Commission can do. Voluntary collaboration is another tool and how can we balance sticks like the standards or mandatory rules -- you know mandatory things we put in interconnection agreements, with carrots like market structures to get what we need on the grid. You know which of our tools should we be using to get from here to where we need to be in the future.

And thirdly, I want to focus on resilience, and I know the afternoon panel is really bore in on that. Resilience seems to be the word of the day. Sometimes I think it means different things to different people. To me, resilience means the ability to recover if something bad

happens.

That true, you try to have resilient kids when you're raising children. I like to brag that FERC is resilient because we've been through a lot in the last several months, in the last couple years, and so an institution can be resilient and the grid can be resilient if it can recover if something bad happens. So we talk a lot about the solution against all hazards is building up the resilience, and I don't like to say "resiliency." I know some people put a "Y," but we don't have time for that.

The resilience of the Bulk Electric System does it come from design? Should we be designing it in a different way to build in more redundancy or optionality or ability to island? Does it come from our spearing strategy, things like grid assurance and building on that? How about standardization? There's a law that I have to mention that at every Reliability Tech Conference. If we had more standardization of design and equipment it would be more resilient. And those are some of the things I want to talk about this afternoon. How we really build up resilience, whether we're talking about GMD, EMP, cyber, or anything else. And of course, in all of these cases how can FERC support it.

There's going to be a lot of competition for airtime at FERC, but reliability is job one and this will be

one of the first things we're talking to our new colleagues about and hopefully we'll have some ideas coming out of today about what the priorities should be. Thank you very much.

MR. BARDEE: Thank you Acting Chair LaFleur. Commission Honorable.

COMMISSIONER HONORABLE: Thank you, Mike. Good morning everyone. I was mentioning to a couple of gentlemen before we started that this is our annual reliability party and I'm glad that you all attended.

I noticed we don't have as many people as we had at our markets tech conference, but that's okay. What we have here today are the people who are very serious about this work, who are committed to, and we're going to roll up our sleeves and be as technical as you would like. So this is the place for energy nerds and geeks, I would suggest.

I'm really glad that we're all here gathered this morning to focus on what I call the bread and butter of what we do here at the Commission and that is ensuring the reliability of the Bulk Power System. And I especially want to thank Mike Bardee and staff especially for your leadership and hard work in pulling together this conference and leading until our colleagues join us whenever they will join us and I hope it will be very soon.

I'd like to especially mention Lodie White, who

has worked so hard in pulling all of this information together. I want to thank each and every one of our panelists. A number of you are repeat performers and we're grateful for that. Thank you for the work that you do each and every day and also the prospectus that you bring and the willingness that you have to share it with us. I especially want to thank our international colleagues who are joining us. We look forward to that discussion every year.

As I often say, it's a new day here at the Commission and this isn't our parents or grandparents' grid any more. When we used to think about how the grid operated, I believe that we thought more about the cost to produce it. Do we have enough capacity to transmit it where it needs to go? But while those are still crucial issues in my mind, we also have to worry about a whole host of other issues that we may not have thought about 10 or 15 or 20 years ago.

More than ever utilities need to be concerned now with where and how power is moving and ensuring that we have adequate voltage support, frequency response, inertia. And while we always knew that these aspects were important in moving energy with the dynamic shift in resources and differing attributes of increasingly abundant resources, such as renewables, we must pay careful attention to these characteristics now. We also are having to pay greater

attention to ever-changing cyber and physical security threats as well as electromagnetic pulses and geomagnetic disturbances.

Also, we are more focused on technological advancements and diversity of resources, which have both created new opportunities, but I would suggest they're also equally creating new challenges for us and it really requires us to elevate our game, so to speak, but also the ways in which we work together. And that's why today's discussion is so important in my mind, given the profound changes occurring in our electric system, this is an opportune time to take stock of the progress we've made, where we can improve, with a view of what lies ahead.

The NERC's 2017 State of Reliability Report -- thank you, Gerry and colleagues -- raises a number of issues for us to consider and I look forward to hearing from our panelists about what's working well and more importantly, what we can do better. This isn't a time, in my mind, for us to come together and pat ourselves on the back. It's a time for us to take stock of where we are and more importantly, where we need to be and how we get there together.

I want to take a moment, if I might, to thank Gerry, Janet, Marcus, Mark, and all of our colleagues at NERC for the dedication that you bring each and every day

and all the regional entities who carry out this important work so well. I've greatly appreciated in my tenure here the opportunities to visit with you, Gerry and your team, but also to spend time at NERC MRC and board meetings, which I admit were a little overwhelming my first time; but also at CERC's meeting with reliability first. Sitting in on MISOP's discussions at SPP, and with CERC, and I've been delighted to host a number of you here at FERC, including the MRO, WEK, PEAK, and others.

Thank you most of all for taking time to educate us and letting us know about the current state of play, but I also see the fruit that this labor brings and I see that we've increased our levels of coordination and decreased MISOP's, we'll hear about that today. We have a stronger focus on cybersecurity and physical security and a greater level coordination among stakeholders in the NERC process and in our working relationship with NERC and I'm really grateful for that and I want to thank you all for exhibiting such a strong commitment to this work.

But we know that our work is not done. We must continue to remain vigilant, to be nimble, responsive, and to remember that no matter what the industry looks like in the future our jobs at their core remain the same, to ensure electricity is delivered safely, reliably, and affordably to the consumers that we serve.

I hope that throughout this day, and I thought it was interesting that yesterday was the summer solstice and the longest day of the year. I wish this meeting was yesterday because we never have enough time to cover all the things we want to talk about, but I'm particularly interested in, and I mentioned to Pat Hoffman before we began, three key areas that I think we need to pay attention to going forward.

Number one is cybersecurity. And I know that's a priority for so many of you, but I think -- and I think everyday consumers are more aware of how cyber threats are growing and evolving and it really requires a new level of awareness education and commitment and an ability to defend our facilities and resources.

Number two is gas/electric coordination. I think as we're seeing such a dynamic shift in the energy mix -- and I applaud FERC long before I arrived -- focus on gas/electric coordination. And when I was a Commissioner along side Chair Haque, we engaged diligently with our FERC colleagues on the issue of gas/electric coordination. That issue will only become more challenging for us, I suggest, going forward.

Last, but not least, is an area that I've seen really resonate in the pre-filed comments that we will hear about today during the tech conference, and that is our

state and federal coordination with our regulatory colleagues. I especially want to thank our colleagues at NERC. Thank you, Chairman Haque. My goodness, you're wearing many hats as you elaborately stated in your comments. We need for our state colleagues to be right there at the front lines with our federal colleagues in carrying out this important work. And I look forward to our discussion today. Thank you.

MR. BARDEE: Thank you, Commissioner.

Now we'll turn to our panelists for their opening remarks, starting with Gerry Cauley.

STATEMENT OF MR. GERRY CAULEY

MR. CAULEY: Thank you. And good morning Chairman LaFleur and Commissioner Honorable and I guess virtual Chairman Bardee for today and FERC staff and fellow panelists.

I want to thank the Commission for holding this annual Reliability Technical Conference to discuss reliability results and priorities. I'd like to offer my thoughts on four key points from NERC's fifth annual State of Reliability Report, which was issued this past week.

First, low power system reliability remains very high. It continues to show year over year improvement. Industry has been very responsive to our risk-based approach and has been shifting resources to fix the most critical

changes to reliability. In 2016, we once again saw no category four or five events and only two category three events. Equipment failures continue to have the highest positive correlation to outage severity or impacts. Relay miss operations and human error are second and third. The number of transmission line device failures and human error reports in 2016 both increased, although the impacts of each declined. We believe the increase in reported incidents is due to better cause analysis, which also resulted in the corresponding reduction in reporting of unknown causes.

The reduction in relay miss operations continues to be very encouraging. 2016 saw the miss operation rate decline from 9.5 percent to 8.7 percent. A second point is that I believe NERC standards and risk-based compliance are having a positive impact on reliability. On June 18, on Father's Day, we passed the 10-year anniversary of mandatory standards. These standards have had a major impact on reducing risks in areas such as vegetation management, situation awareness, operator training and system planning and modeling.

Over time, we've seen a dramatic decline in the number and the severity of compliance violations. I believe, however, it may be time to focus again on streamlining the requirements to ensure the investment and compliance is commensurate with the reliability gains. We

also want to continue working to ensure that compliance becomes integrated into reliability operations and is not seen as a separate administrative burden.

A third point is that changing technology and resource mix are reshaping reliability at a pace we've never seen before. We've seen the introduction of digital technology operating in microseconds being integrated with traditional protection and control systems that operate in cycles and seconds.

A clear example occurred last August 8, 2016, during the Blue Cut fire in California. In the past week, NERC published a technical paper and a Level 2 alert describing how 1200 megawatts of solar power quit producing at a critical time because the invertors were interpreting transit voltage and frequency values from line trips as the actual system frequency and voltage. I want to applaud the recent response of the California ISO to require additional reserves in the market to address uncertain response from some inverter-based resources.

NERC has been working with renewable vendors to adjust inverter settings and to provide effective ride through capability and the vendors, I assure you, are being very cooperative with us on this issue. I also feel we may need to clarify our standards to ensure that when new technology gets introduced into the system that the

terminology that we used to think was fine is clear with regard to the new technology.

We're also focused on a number of other emerging reliability risks and I'll leave those primarily to Mark Lauby on the next panel, but they are the impact of distributed energy resources on the Bulk Power System. The dependence on natural gas, particularly, critical storage and pipeline facilities, and the adequate provision of essential reliability services when large rotating machine which used to be base loaded are now not being dispatched.

My fourth point is that cybersecurity has become the most important risk that we face. Today I believe we've seen exceptional performance with no electrical system outages or serious events, but as we will hear in a later panel from Mark Sachs the threats are becoming more serious and at an alarming rate. The 2015 and 2016 attacks in the Ukraine show that the tools for nation-stayed disruption of power grids have been fully developed and tested.

The recent announcement of crash override, a very robust threat to industrial control systems and operating systems, is of very serious concern to me. NERC issued an alert to industry last week with proposed mitigating measures for industry. Wannacry and the Internet Things attack in recent months are also likely to affect us, but more in the corporate side, but those threats remain

serious.

I want to thank you for your time today and I very much look forward to your questions. Thank you.

MR. BARDEE: Thank you, Gerry. Next, we have Patricia Hoffman from the Department of Energy.

STATEMENT OF MS. PATRICIA HOFFMAN

MS. HOFFMAN: So thank you Chairman LaFleur, Commissioner Honorable and the Commission staff. Thank you very much for your leadership. Good morning and it is a pleasure to be here to participate today at the technical conference on the state of electric reliability. I appreciate the opportunity to express the views of the U.S. Department of Energy.

As Gerry has mentioned, the U.S. electricity sector is in the midst of major changes and I see little reason to expect that this process will slow down or that we will reach some new equilibrium any time soon. On the contrary, the process of change that we are experiencing today will probably continue. Accordingly, I think the fundamental challenge is now to understand this process and to manage it with proper investments so that our nation's electric infrastructure remains reliable, affordable, and secure.

Before I highlight some topics of concern for this Commission, I would like to take a moment to reflect on

some accomplishments by industry that are providing value to system reliability. Lessons learned from the 2003 blackout highlighted the need to develop better, real time tools for operators and reliability coordinators, improve system modeling data and data exchange practices, require the use of real time synchronized data recorders, and tighten communications protocols, update communications hardware where appropriate.

Lessons learned from the 2011 Southwest blackout highlighted the issues from planning, modeling, and remedial action schemes. Recent hurricanes have demonstrated the need for improvement in communication, automatic switching, and outage management systems. A significant amount of research development and deployment has advanced most of these recommendations, including the development and deployment of PM used, advanced meters, outage management systems, real time tools for operators, but unfortunately, there are still some recommendations that are still under development, such as dynamic remedial action schemes, improved and faster modeling systems with great fidelity.

The Electric Sector Coordination Council reiterated the need for improved communications and redundancy in communications, but as Gerry has stated, the performance of the system is improving overall; however, one must keep close watch on regional issues developing. So

with respect to this panel today, there are a couple of things I'd like to highlight.

Physical and cybersecurity, utilities and system operators need to continue the efforts to identify data, facilities and systems that are essential to the reliability of the system and take reasonable steps to harden them. Mitigate the reliability risks associated with rising gas and electric interdependence. The Aliso Canyon Event involved the functional loss of a major underground natural gas storage facility in Northwest Los Angeles, which has lead to increased reliability risk to the Los Angeles area.

The third area is the need for planners to build more flexibility in optionality into their systems, both in the short term and the long term. The uncertainties the assistant planners must take into account have multiplied in recent years and this condition is not expected to change any time soon.

With respect to data and data analytics, without sustained data and visualization, long-term grid reliability can be compromised. With respect to diversity of generation and reliability, the electricity grid has undergone a transformation as new technologies, changing economics, and shifting customer behaviors and government policies are driving change and we must identify the services expected from the generation fleet in the United States and the

appropriate compensation. So with respect to distributed energy resources, the trend is going towards more decentralized electric grid with greater variability of resources providing powers in the ways that today are much less predictable, hence, the ERs are challenging to our traditional approaches to planning operations and raise new questions about how to control, coordinate, and optimize a large number of diverse resources.

And the last thing I'd like to mention is the reliability study. Earlier this spring, Secretary Perry asked DOE staff to initiate an internal study to explore the issues central to protecting long-term reliability of the electric grid. Secretary Perry asked the staff to explore three issues: the evolution of wholesale electricity markets, including the extent to which federal policy and the change in electricity fuel mix challenge grid reliability, whether wholesale capacity markets are adequately compensating attributes such as one-site fuel supply and other factors strengthening grid resilience and the extent in which regulation and legislation affect early retirement of base-load generation plants.

While recommendations are expected from the final report, it is likely that several areas related to reliability will be identified for further research and study. So with that, I'd like to conclude my comments and

thank you and look forward to questions.

MR. BARDEE: Thank you, Pat. Next, we have Chairman Asim Haque from Ohio.

STATEMENT OF MR. ASIM HAQUE

MR. HAQUE: Good morning. Chairman LaFleur, Commissioner Honorable, and staff, thank you for inviting me to participate in today's technical conference. My name is Asim Haque and I am the Chairman of the Public Utilities Commission of Ohio. I have the privilege of serving on the Board of Directors of NARUC and I'm also one of two state government sector representatives elected to the Member Representative Committee of the NERC, actually an opportunity that was provided to me by then-President Honorable. So thank you -- I think thank you.

It is in this total capacity, Chairman of the State Commission, representative of NARUC and of the NERC MRC that I present these remarks today. These remarks are meant to simply inform the Commission on topics related to NERC's reliability endeavors that are foremost on the minds of the states. These topics include distributed energy resources and their collective impact on the Bulk Power System, reliability impacts associated with the retirement of base-load resources and efforts to incorporate costs into the NERC's standards process.

Before I elaborate on these topics, I would like

to first recognize the diligent work of NERC. NERC has the difficult and highly technical task of ensuring the reliability of the Bulk Power System and it performs very admirably in that task. State commissions also appreciate the strong relationship we have developed with NERC.

The rapid advancement of technological innovation on the electric grid is causing many states to launch grid modernization endeavors. Ohio, in fact, recently launched a comprehensive grid modernization endeavor entitled "Power Forward." Power Forward is built upon to pillars, innovation, both technologic and regulatory, and the concept that this innovation must serve to enhance the customer electricity experience.

As the PCO has learned in Power Forward, innovation associated with distributed energy resources is quickly growing and we expect for this marketplace to continue to expand. Regardless of the path the states take for integrating and compensating these resources, the states understand that they are traversing through somewhat uncharted waters. This sense of the unknown also applies to the intersection of distributed energy resources and the Grand Pack Dunball Power System reliability.

NERC understand this and has proactively created the Distributed Energy Resources Taskforce. NARUC is pleased to be actively participating in dialogue with

members of that Taskforce. They believe that the recommendations in that Taskforce's final report associated with things like data sharing, modeling, and industry collaboration are very, very sensible.

The states understand that the increased proliferation of the distributed energy resources cannot compromise bulk power system reliability. The states and NERC are learning together and the states stand ready to assist. This could take the form of information sharing so that appropriate modeling can be conducted for the recommendation of that Taskforce report. This could also take the form of an effort that produces some type of uniform guidance socialized through NARUC.

There continues to be much dialogue surrounding the changing resource mix and the retirement of coal and nuclear generating plants. Some states are taking measures to subsidize these base-load plants through various state initiatives. These state initiatives have prompted very robust policy debates. Missing from this discussion, however, has been a true scientific analysis to explain reliability risks to the Bulk Power System as these base-load units face potential retirement.

NERC is uniquely situated to conduct this analysis, as the electrical liability organization for North America NERC is capable of examining this issue through

actual science and engineering. NERC conducts special assessments on emerging issues and trends that will influence both power system planning, development, and system analysis and this is one of those items that NERC is considering studying.

Grid reliability should be viewed as a scientific problem and NERC's concept of a special assessment for accelerated base-load retirements could provide concrete data that may serve to inform public policy determinations, thus, NARUC would support and encourage NERC's efforts to engage in collaborative discussions based on the scientific outcomes of that study.

I previously testified that cost should be considered in NERC standard development and implementation and that this would help to foster a culture of reliability excellence. The cost of facility compliance with NERC reliability standards will always be a concern. For state commissions, I am pleased to report that NERC, based on input from its stakeholders, including NARUC, has developed a plan to promote cost analyses in its standards process. NARUC has requested that NERC provide meaning reporting related to the outcomes of these endeavors at least biannually. After NERC's latest proposals are initiated, we would like to know how these actions are tangibly impacting the -- process, if at all. But again, NERC has done a

marvelous job in addressing this.

Commissioners and fellow panelists, thank you again for the opportunity to participate this morning. I look forward to questions.

MR. BARDEE: Thank you, Asim. Next, is Charles King, testifying on behalf of EEI.

STATEMENT OF MR. CHARLES KING

MR. KING: Thank you and good morning. Acting Chair LaFleur, Commissioner Honorable, staff, for the opportunity to be here this morning. Just a brief perspective that I think is important when we have these conversations, electricity's value is measured by its reliability. The significance of reliability has not changed significantly since the times of Thomas Edison first opening the Pearl Street Electric Station in New York City up through the technological advances that have lead us to the modern electrical grid today marked by things such as renewables, distributed generation, smart grid tools that include energy response and then also ideas that were once aspirations of how we would use electricity that are today reality, such as electric vehicles.

However, those innovative transformations, as we all know, that are a part of the electrical grid today have also brought forth challenges to reliability as we've already discussed this morning, and that includes providing

essential reliability services and also, of course, cybersecurity as two of the largest.

I'd like to underscore that when we discuss reliability it's essential that we keep in mind the industry incentive fostered by the very nature of our business. It's simply in our DNA to provide reliable sources of power and deliver that power reliably to our customers each and every day. With or without mandated standards, the industry is focused on providing reliable power. Now the reliability standards are in place to provide a strong regulatory framework that promotes and works to support reliability.

The Commission, NERC, and the industry, I think, have done an excellent job at building and implementing that framework as evidenced by the current high levels of reliability. The reliability risks take on many forms, shapes, and sizes. For example, cybersecurity every day it evolves. It exploits known vulnerabilities, unknown vulnerabilities and we also have innovations, such as those I mentioned a moment ago that give us distributed energy sources.

But as good as the regulatory and standards framework is at promoting reliability and addressing challenges and threats to reliability, the speed at which these risks and threats are evolving creates concerns. Cybersecurity, for example, the threats evolve literally

every day and the process and time it takes to develop a standard and implement a standard may not yield the desired results to mitigate vulnerabilities in a timely fashion.

Today's grid technology continues to rapidly evolve, such as smart inverters. Sometimes those underlying reliability risks cannot be identified and mitigated as quickly as desired, which makes drafting reliability standards and requirements difficult without the time for effective study and cooperative research. While the standards development process is solid and effective, its design does not easily accommodate these emerging, evolving risks that we face today.

In light of this limitation, we need to seek out ways to supplement our current processors and other alternatives. Many in government and the industry, however, have already stepped up to this challenge, for example, the work done by the Electricity Subsector Coordinating Council recently in the area of grid security. The definition and roll out of the cyber mutual assistance model I think is an excellent example of that partnership. That partnership, by the way, between industry and government does not replace the current regulatory and standards development process. It simply offers an alternate path to expedite response and further strengthen the grid.

We encourage the Commission to look for

alternatives to prescribing new or burdensome regulations to addressing these emerging reliability risks. Grid technologies and the reliability risks associated with them are going to continue to rapidly evolve, too rapidly to address them through prescriptive requirements.

The Commission, NERC, and us as industry, we all have a shared commitment to reliably operate the Bulk Power System. That's evidenced by ongoing work to address reliability, improve reliability through regulation, government/industry partnerships, applying lessons learned from events in North America and around the world, and also just the rigor with which we approach addressing new challenges caused by new technology and emerging threats.

So in recognizing industry's responsibility to our shared commitment to sustain and advance reliability, we'll continue to partner with the Commission, bring forward possible solutions, alternatives, different approaches and we look forward to collaborating with the Commission, NERC, and our other stakeholders to discuss these possible solutions as we all work together to protect and advance the reliability of the grid. Thank you.

MR. BARDEE: Thank you, Mr. King. Next, we have Steven Wright, speaking on behalf of the Large Public Power Council.

STATEMENT OF MR. STEVEN WRIGHT

MR. WRIGHT: Thank you for the invitation to appear again today at this conference. We reviewed today a unique law that assumes effective collaboration and communication between industry and government. Through focusing annually on the most strategic issues, this conference is an important element of making the law successful.

I want to start from the perspective that (mic malfunction) -- , managing a number of systems that I've had responsibility for adopting those standards.

To get to the first two points that Acting Chairman LaFleur laid out, we have four primary suggestions for strategic focus for the next year. First, create more compliance management rewards for entities that embrace a risk-based approach to reliability standards. The standards are appropriately a systematic, methodical means for managing a very complex system

In the case of our utility, and I believe most around the country, our compliance management staff and costs continue to grow. Our challenge since the time this conference was originally initiated is how can we get the biggest bang for our buck. The NERC risk-base compliance and monitoring enforcement program encourages utilities to perform inherent risk assessment to better understand impacts the entity has on the Bulk Electric System. And

the CMAP also encourages an assessment of internal controls that an entity has in place to manage reliability risks.

At Chelan and for many of my LPPC colleagues, we chose to go all in on IRA and ICE. There is no doubt in my mind that the resulting knowledge and process management has improved our impact on the reliability of the system. And in fact, our auditors identified us as a top tier performer. What I had expected, though, was that as we better understood and documented our contribution to reliability there would be reductions in compliance management costs.

Now in fact, our audit scope was reduced by 87 percent, making data process go smoother. To this point, though, there has been little reduction in our documentation requirements, which is where the bulk of reliability management costs occur, of the 1,236 requirements and sub-requirements applicable to Chelan four have been identified as eligible for self-logging.

NERC has proposed process modifications that could lead to more rewards for utilities that choose the path of seeking excellence and we encourage FERC to respond positively to these initiatives. We also would suggest that the regions be given more authority to say don't worry about where individual entities' standard implementation is not material to Bulk Electric System reliability.

Second, the use of cost-effectiveness criteria,

NERC is to be commended for their efforts to advance this concept. A lot of good work has been done. But as a knowledgeable friend of mine recently summarized, it's difficult and we still have a long ways to go. We would encourage further dialogue between industry and NERC and FERC to advance these concepts.

An important issue to arise this past year has been supply chain procurement. LPPC believes this problem is real and must be addressed and it's good news that the industry has recently approved a new standard. I'm concerned; however, that fundamental management principles and accountability are at risk of being violated by managing this challenge only through the statutory framework of mandatory standards that apply solely to the electric utility industry. An entity can only reasonably be held accountable for actions that they can control and I would strongly encourage that FERC, NERC, and the industry jointly approach other federal agencies that have cybersecurity responsibilities to develop an overarching strategy that extends beyond the electric sector.

Fourth, any discussion of reliability would not be complete without considering the changing nature of the physical operation of the Bulk Electric System, particularly, in the West were there's a proliferation of variable energy resources. The challenge of managing a

system with increasing amounts of non-dispatchable resources has been understood since at least 2013, but the pace of BERs being added to the system is accelerating beyond previous projections. Actions are being taken and near-term reliability, I believe, is likely not at risk, but as the fleet and grid transform metrics such as a resource adequacy need to evolve.

At this point, solutions beyond the next three to four years addressing in particular the afternoon ramp challenge are not agreed upon or being executed. And we also have to consider alternative means of compensating for needed flexible capacity.

So in conclusion, we should be proud that reliability is getting better, but as with any system there are opportunities for continuous improvement. We commend the Commission for holding this conference on an annual basis and look forward to continuing to work with you.

MR. BARDEE: Thank you, Steve. Next, we have Dr. Babak Enayati from IEEE.

STATEMENT OF DR. BABAK ENAYATI

DR. ENAYATI: Thank you. Good morning Chairman LaFleur, Commissioner Honorable, FERC staff, and my fellow panelists. I thank you for the opportunity to speak at this conference today. IEEE is the world's largest technical

professional organization dedicated to advancing technology and IEEE and its members inspire global community to innovate for a better tomorrow for its more than 420,000 members in over 160 countries in its high cited publications conference psychology standards and professional and educational activities.

As the most active IEEE society in publishing standards, IEEE Power and Energy Society provides the world's larges forum for sharing the latest in technological developments in the electrical power industry and so various policies, regulations, and legislation seek to deliver the environmental objectives for the power generation sector. The North American Electric Power System is becoming more reliant on wind, solar, natural gas, and demand response.

In addition to changing energy landscape in the wholesale market, most of the states in the U.S. have ambitious goals to deploy DER in the retail market as well. Given that DER penetration, including green -- generation is increasing rapidly in the U.S. The impact on the Bulk Power System reliability is becoming more apparent.

In order to avoid reliability violations, supply disruptions, or extensive transmission upgrades, DER interconnection standards need to be updated to allow DERs to support the Bulk Power System during frequency and bulk disturbance, also known as ride through capability. As

deployment of DERs on the distribution system increases, the impacts on the Bulk Power System reliability need to be addressed promptly by updating the standards that govern the technical aspects of the DER interconnections.

Many utility distribution companies in the U.S. have adopted IEEE 1547 standards, which provide a set of technical requirements that each DER shall meet to interconnect to the distribution electric power system. Given that the implementation of IEEE 1547 standard is essential to the Bulk Power System reliability, there are some major challenges associated with the implementation of the standard.

The top two concerns are, number one, modeling. Currently, the tools that are widely used by distribution for utilities for DER interconnection protection studies are not capable of accurately modeling the DERs with the grid support functionalities, also known as advanced DERs.

Number two, concerns related to adverse impact of advanced DER functions on the distribution system anti-island protection and short circuit fault detection. Some distribution utilities are concerned that the advanced DER functions may have adverse impact on the distribution system protection related to the prolong fault and island distraction due to the ride through requirements.

What needs to be done? As the IEEE 1547

standard is in the revision process, IEEE recommends that the Commission collaborates closely with the distribution utilities, the original ISOs to resolve the concerns associated with implementing the DER ride-through requirements. This collaboration will avoid the delay to implement the IEEE 1547 standard once it's officially published. IEEE believes that the Commission and NERC can play a key role in directing those discussions through the regional ISOs.

IEEE Power and Energy Society has the resources and the technical knowledge to help the Commission, NERC, and the regional ISOs to implement the industry standards related to Bulk Power System reliability. And I also want to give you the good news that the 1547 standard passed the ballot last Sunday. So it was open for ballot for a month and it passed the ballot. They are forming a comment resolution team and will address the comments that we received. It was in total about 1,457 comments, so yes, we'll work on those comments and we're targeting the end of this year, hopefully, to publish the standards.

So this concludes my presentation. I will be happy to address any questions you may have.

MR. BARDEE: Thank you, Doctor. Next, we have John Twitty from the TAPS Group.

STATEMENT OF MR. JOHN TWITTY

MR. TWITTY: Madame Chair and Commissioner Honorable, nice to be here today. Mr. Bardee, thank you very much for the opportunity. I am here today to speak on behalf of TAPS. TAPS is an organization that represents transmission-dependent utilities in 35 states. The members of TAPS are joint action agencies and utility operators with direct responsibility for keeping the lights on for their customers.

Because we are transmission-dependent, we are highly reliant on the reliability of transmission facilities owned by others and at the same time many TAPS members are subject to compliance with NERC standards. So we are both supportive of cost-effective actions to ensure bulk system reliability and acutely aware of the increasing cost of new reliability regulations.

I've been in the business now in my 35th year and have experienced two municipal utilities and now at TAPS. I also have the privilege this year of serving as the Chair of the NERC Member Representatives Committee and I was a member of the NERC Reliability Issues Steering Committee. So collectively, this experience has provided me lots of thoughts about customers and reliability.

Let me began by acknowledging the success that FERC and the ERO have had over the past decade and a little bit more. We've collectively kept cascading outages to a

minimum through a period of rapid change in the industry and with technology and I suspect everybody agrees those changes aren't going away. I believe it is important to emphasis that we must be careful to measure reliability against what the Congress wrote.

Outages occur for a variety of reasons, of course, but Congress directed that FERC and its ERO guard against BPS instability, uncontrolled separations, and cascading outages. This focus is particularly important to remember, especially as distributed energy resources begin to play a greater role in today's grid. We must be sensitive to avoid allowing the federal jurisdictions of FERC and NERC to creep into local distribution systems of the operating utilities across America. It should not be the intent of FERC to undercut state and local regulatory mechanisms that are best designed to serve the need of local communities.

I would also like to discuss the cost associated with the requirements of standards that have implemented since they became mandatory with passage of the Energy Policy Act of '05. When I served as general manager of City Utilities, I used to say to our industrial customers that we could guarantee 100 percent reliability, but they wouldn't want to pay that much. The engineers in the room always used to say you really can't do that and we might all agree

about that, but the point is the higher degree of reliability delivered the higher the cost.

We all understand the importance of competitively prices energy and its impact on the competitiveness of our customers. After all, it is the commercial and industrial customers we serve who provide jobs in our community. I also think we need a renewed paragraph 81 effort. When FERC first suggested that requirements and standards be reviewed to make sure we weren't duplicating effort or undertaking efforts with little benefit, it was a welcomed sign.

Earlier this year, Gerry Cauley mentioned that very thing and we support it in the strongest possible terms. Once that first effort was underway, we were hoping there could be a significant number of requirements that could be retired. And while there are successes to be celebrated, we believe there are even more requirements and standards that should be carefully reviewed to see how much value they bring.

Let me close by stating the obvious, cybersecurity and cyber issues, generally, have given us perhaps a greater threat than any we face. Many positive steps have been taken to help address these issues with the EISAC and ESCC working actively to help prevent widespread outages. Again, TAPS is most supportive of these efforts,

but we must be careful about the costs associated with this work and carefully examine whether tools available to FERC and NERC other than reliability standards are better suited to promptly addressing evolving cybersecurity threats taking full advantage of quickly changing technology and lessons learned.

Again, thanks so much for the opportunity to be here today. Look forward to the conversation.

MR. BARDEE: Thank you, John. And finally, we have John Hughes from ELCON.

STATEMENT OF MR. JOHN HUGHES

MR. HUGHES: Thank you Michael and Commissioners. It's a privilege to be back here. And on behalf of my members, I want to state that a few things are as important to ELCON members as reliable electric service. They can't do business without impeccably reliable service.

I also want to start on a positive note by thanking the leadership of the ERO Enterprise for the access that they've given to large manufacturers and particularly NERC staff, the very capable Board of Trustees and the regional entities. I think I can state that NERC is no longer a utility club.

I especially want to compliment NERC and the regional entities for adopting results-based standards development and the risk-based approach to compliance

monitoring and enforcement. This has significantly reduced a regulatory burden of NERC standards on our members that are registered entities and is also, I believe, prevented frivolous registration by members that provide no risk to the reliable system.

ELCON members have a unique perspective on reliability issues. Our definition of reliability is much broader than what was in Section 215 and by that I mean that we are subject to the dual jurisdiction of states as well as the federal laws and many manufacturing facilities are interconnected that both the BEF system as well as the distribution system and events on either one of those systems can impact the manufacturing process.

We have an overriding concern about the current changes in the industry with the adoption of more intermittent resources and DER distributed energy resources, but we are grateful for the fact that at least at the BES level NERC is addressing these concerns and we hope that the Commission will support these efforts by NERC.

With the remainder of my time, I want to focus on two specific areas of concern. First, in the interest of the canary in the mine shaft, several of my members are reporting an increase in power outages that do material damage to their manufacturing facilities. And I don't have enough degrees of freedom of data on this to really

definitively identify a trend. They seem to be scattered throughout the United States and the best I can tell they're kind of 50/50 at both the BES level and the sub-BES level.

While I'm continuing to work with my members to try to identify more specifically what's going on, obviously, these are not associated with any type of wide, cascading outage. These are all local events. I keep hearing from quite a few of my members that they're experiencing greater voltage problems outside the fence of their manufacturing facilities. Of particular concern is they're getting no feedback from their local utility on what's causing these problems.

A second concern deals with a trend that there's an expectation that manufacturers should have their manufacturing process dispatched for the purpose of providing BES reliability and they can't do that. There's a term called "demand flexibility" that's used by advocates of a carbon-free society to explain why they think that it's really the customers that should be providing the reliability to the system rather than utilities.

We disagree with that mindset. Most manufacturing facilities, especially large ones, are inflexible. And I would note that NERC has -- excuse me, FERC has a NOPAR pending on primary frequency response which

goes down that path and we would like to see a speedy resolution of that issue.

And again, thank you for the opportunity to appear and I look forward to your questions.

MR. BARDEE: Thank you, John. Thanks to all of our panelists. Let me turn first to Acting Chairman LaFleur for questions she may have.

CHAIRMAN LA FLEUR: Well, thank you Mike and thank you to all the panelists. I love this seat. I'd rather sit where Mike is sitting, but we have a great view here.

Okay, so many ways I could go. I think I'm going to start with the question I posed in my opening comments and was also raised by Steve Wright's comments. And I want to call out Steve Wright as my memory being the person who suggested having these conferences in 2010. So in some of your comments at that time, if I recall, about more interaction with Commissioners and so forth, so thank you.

Steve, John, John Hughes -- John Twitty and John Hughes all talked about I'll call it risk-based selective enforcement of standards and being more risk-based in the way we conduct compliance with compliance -- whatever CMEP stands for, Compliance Monitoring Enforcement Program. And I tried to be supportive of NERC's desire to be more

risk-based in enforcement, but I had this competing feeling of like why do we have standards that we don't want to enforce?

If there are standards that don't relate to -- that are, in Steve's words -- we should remove from the list of standards if you've had this inherent risk assessment standards that are needed for grid reliability. If you have standards that are not needed for grid reliability, why are they standards?

Are there things -- are there documentation of other standards you would propose streamlining because it comes out as like after the fact to kind of only selectively enforce, but then you always a fear you might be enforcing the wrong ones or the mechanisms you use to figure out what to enforce with whom are not sufficiently sensitive. So is there a problem with the complexity of the standards? Is there something we should do 11 years in to adjust this rather than backing off on enforcement?

And I'll maybe start with Steve, but by Gerry or anyone to comment.

MR. WRIGHT: I think there are two ways to come at this. You know one is very consistent with what Gerry's talking about and one is a bit new.

So a few years ago, I can't remember exactly how many, NERC were through the paragraph 81 process to review

all the standards and a couple of the panelists here and Gerry, I think, said there may be time to revisit that and see where we can get and that was as useful exercise. I described it as modest, but significant changes that were made to the standards at that time to review and understand just what's working and what's not providing as much value and it could well be time to review that. It depends on which standards you're talking about. I don't that we're really quite ready on cyber standards yet. We're probably a year or two away.

CHAIRMAN LA FLEUR: I would agree.

MR. WRIGHT: So you have to look at where the standards are in terms of their maturation process and then decide whether it's time to go through that paragraph 81 process.

The part that I'm suggesting that's a bit different is we put in place IRA and ICE in order to be able to understand the impact of each registered entity's impact on the Bulk Electric System. And that has really been good work. I have to tell you it was hard. It was very difficult, but I think it was extremely valuable to do that. But now what we have is the opportunity to look at each registered entity and standards are one size fits all. And now with IRA and ICE, we have the ability to look at the impact each registered entity has on the Bulk Electric

System and determine whether the one-size-fits-all standard is necessary in terms of its full application to that entity or not.

In order to do that, it would require more authority to be given to the regions because there's no way, I believe, that NERC could be able to manage that process for all of the registered entities, but just take a look and say, okay, do we need the full application of this standard for this entity, given some entities are at that big impact and others have a much smaller impact.

CHAIRMAN LA FLEUR: Well, I fully supported the paragraph 81 effort, which I think Commissioner Norris first suggested, but I thought of that as much more kind of looking through and making sure we didn't accidentally have duplicates or there were little things we could shave at the edges.

I just want to understand. Drawn to its logical conclusion, Babak, who is sitting next to you, from National Grid, would have a different set of standards or Southern would have the highest standards because they're bigger and someone little would have fewer standards. Is that kind of what you're saying?

MR. WRIGHT: I don't think it's necessarily bigger or smaller. This is the great thing about inherent risk assessment. It allows you to look what the impact of

the particular facilities that you have what's their impact on the Bulk Electric System, so it could be that you might be a small entity, but you could have a big impact on the Bulk Electric System.

CHAIRMAN LA FLEUR: So if you don't have a big impact, then we loosen up on something we might require someone else to do, in concept.

MR. WRIGHT: And it wouldn't be tied to the entity itself. You'd have to go through standard by standard, right? So it could be that the individual piece -- you know go back to the Southwest outage. Clearly, there were facilities on the IED system which were really important to the Bulk Electric System.

CHAIRMAN LA FLEUR: I thought of them when you said that.

MR. WRIGHT: I think we probably all do candidly, is thinking through that, so you wouldn't be able to say, okay, you're a small guy; therefore, you have no impact. You'd have to go through and say what is that facility that you have? How does that relate to the standard? How important is that to the Bulk-Electric System?

CHAIRMAN LA FLEUR: So you're talking quite a bit of customization of the standards.

MR. WRIGHT: Yes. And that's why I said would

require authority to be given to the regional entities in order to be able to go through that. I don't think that could be managed ^^^^

CHAIRMAN LA FLEUR: So think paragraph 81 is enough to do any kind of macro streamlining we need to; that that's enough of a tool.

MR. WRIGHT: So our experience with paragraph 81 was a favorable one. I think it worked well. And again, that's probably something that should be repeated every so often to just to go back through and say how has the system evolved and what have we learned.

CHAIRMAN LA FLEUR: John?

MR. TWITTY: Well, Madame Chair, I think it's important to continue that paragraph 81 effort. You know when it first started there was lots of enthusiasm with that and I would certainly agree with what Steve has said here.

The intent then, as I understand it, Gerry certainly can correct, is that we would move that process to where were writing new standard. We're writing them with the thought that we're going to review what's in the field of vision and in that process we're going to make sure that going forward we're not duplicating, that we have cost-effective standards.

I really would be supportive and I think TAPS would be supportive of sort of a renewed effort to start all

over again. I think Steve's comments about internal controls and inherent risks is particularly important for TAPS because we're small members, by and large. And I say often our members might do something that might turn the lights out all across town, but it's not going to feed into the Bulk System. You may catch heck at the grocery store or church next Sunday.

CHAIRMAN LA FLEUR: Or when you see John Hughes.

MR. TWITTY: Yeah. Hey, John, the lights are out at Alcoa today, happy to know that, really to tell you why. So I would really like to see a brand new effort and to further recognize that not one size fits all.

CHAIRMAN LA FLEUR: John Number Two.

MR. HUGHES: Briefly, one of the nice thing the NERC does -- actually, it's something that its Board does is seeks policy input from the MRC and on a quarterly basis in advance to the Board members. And one of the recommendations that we put forward recently I think touches on what you're getting at, and that is we need some sort metrics on the requirements of each standard that tie the requirement to the quality of the reliability or improvements in the reliability. And I think it's safe to say that no standard is written perfectly and if we had more time and more people to work on them we would want to improve them. But maybe a metrics of this type might be a

way of identifying which ones could be rewritten for more effectiveness and really identify and truly reduce the risks.

CHAIRMAN LA FLEUR: Gerry.

MR. CAULEY: Thank you. I appreciate the comments that fellow panelists in wanting to streamline and get more efficient around compliance and standards.

One of the pivots that we're in the process of making is probably not widely known, but we're preaching around the ERO Enterprise is risk-based compliance standards is moving to sort of how do you prioritize the most important reliability issues to a new concept, which is basically fearless focus on any effort you can do to prevent the next outage and use the standards for that and use a compliance activity.

So if an activity is not contributing to preventing the next failure, then it's not as helpful. You know so there's some value in standards and compliance for punishment if somebody does really bad behavior. We're making that pivot across NERC and the Enterprise.

So that points out a few things. First of all, I do believe that there's an opportunity now to do a concerted review of the standards to make sure they're all contributing to preventing the next outage.

CHAIRMAN LA FLEUR: By definition, they should

all have something to do with preventing cascading outages on control separation.

MR. CAULEY: Exactly. And given the asymptotic approach, we've seen some good reliability and the crunch on revenue and resources I think it's time to go back and look at it again, not in an incremental five-year process, but maybe one more time look into the review. I don't believe we need to go as far as Steve Wright is suggesting in terms of sort of an optional menu of what's enforceable for different folks. I believe that we legally have and the regions legally have the discretion today to monitor and enforce whichever standards we feel suit an individual entity and that's really the purpose of the inherent risk assessment and really creating a risk profile for each entity.

And I think the regions could continue to do a better job of explaining that and explaining what will be looked at and I think there can be a negotiation between the entity, but I don't think it makes sense to take a North American set of standards and start creating sort of a little checklist matrix for each entity. The standards are the standards, but if you buy in a philosophy of the purpose of looking at anything is prevent the next failure it's going to point you to the ones that are important for that entity in that situation and based on their history and we

have full legal discretion to work on the ones that make sense.

CHAIRMAN LA FLEUR: But isn't it the concept of the standards that any of these things could be a leading indicator of something? You know because you don't know where the next failure is. You know the kind of pyramid of little things lead to big things. So is the concept that someone might find a company violating a standard, but say, well, that one isn't really like to contribute to an outage.

MR. CAULEY: Well, another concept of this pivot is really to get the entities to focus every day on the small things so that they're managing that. So the effective controls within a company to suppress the -- you've been saying this for years. It's a mountain of small things that can actually tip us over, but if we're fighting to suppress the small things on a day-to-day basis, the entities are involved in that, they're aware of that, we're monitoring the effectiveness of their internal controls monitoring. They're self-reporting. They're self-correcting. That helps deal with that sort of sneaking up through a bunch of small things.

CHAIRMAN LA FLEUR: Thank you.

I want to turn to a different hot topic and that's fuel and fuel security. Secretary Hoffman talked about it in talking about the 60-day study. I believe Gerry

talked about Aliso Canyon, which is something we're very closely watching, especially on a day when it's extremely hot in Southern California like today.

Back in -- I think it was 2012 when we first started on gas/electric and I put out like three questions or four questions, I don't remember, to the industry. One of them was how should we address this and one of them was is there something we should be doing with standards. And the immediate reaction was whatever you do this has nothing to do with standards. Don't do standards. But is there something now, as we look at the changes in the system and the decreased reliance on types of technologies that have on-site fuel as an exclusive base load. Should we be changing our planning standards in some way to take that potential loss of the pipeline into account or the gas storage? Is there something we should be doing in -- that NERC should be doing in that area around that issue?

I know there's a market aspect, but there might be a reliability requirement aspect. Something I know Gerry's hinted at for years, but I mean Aliso Canyon brings it, at least, into the front of topic. Excuse me; it was Secretary Hoffman who mentioned Aliso Canyon.

So I'm interested in if anyone thinks that our planning standards or something else should be changed because of the fuel situation we have now.

MR. CAULEY: I could take a first stab. So we're doing a special assessment project right now and I expect the report to be out -- I don't know the exact date, but 30 to 60 days its coming. And it's looking at critical points in that dependence between gas and electric where pipeline failures or we've gone around evaluated the different storage sites and looked at the potential impact of loss of key facilities. And philosophically, putting aside the question of a standard, it would be clear from this report, I believe, that you should be planning for the loss of a most critical, a most impactful facility, including if it's on a gas system

And so I think the answer is it may point to -- once we understand the issue, understand how significant it is, how many places does it occur; but it would be good practice to plan for that loss because you never know it won't happen.

I would go further and probably go out a little bit of a limb, but I think there's a general challenge that we need to step back at a policy level and look at the reliability, dependability, and security of the fuel delivery system on gas, given how dependent we are in so many regions. And I know we don't have any jurisdiction at all in the gas arena, but I know the Commission does.

CHAIRMAN LA FLEUR: Well, we don't have the

reliability jurisdiction over gas, but we have reliability jurisdiction over the people who burn the gas.

MR. CAULEY: Right. I'm not a lawyer, so I'm just making loose statements, as an engineer, but I am concerned that you have certain reliability expectations and standards on the electric system and what I consider a foundational piece, which is the fuel delivery doesn't have equivalent standards or expectations of dependency and reliability and security. I don't have a specific proposal, but I think that that's there to be looked, at in addition to your question, which is do we need to look at our planning and when it's one is now loss of a specific critical gas facility, which I agree with.

CHAIRMAN LA FLEUR: Thank you. Pat.

MS. HOFFMAN: So I look at it that the important thing that the regions and the grid operators need to do is an assessment of the fuel risks to grid operations. And so as looking at the level of regional diversity and to the extent possible how dependent is a region on one fuel source and from that perspective so that it gets to the point that Gerry brought up of really what is the risk to the reliability of the electric system.

But at the end of the day, I know the market operators are really looking at availability and saying that there has to be redundancy in fuel supplies and putting the

onus on the generators to make sure that they have fuel availability as part of providing electrons and electricity to the system and reliability to the system. So I think it can come down to that point of handling it from a redundancy point of view, but also, I think it's important to have a risk assessment done.

CHAIRMAN LA FLEUR: Thank you.

And I'll ask one more question and that's on data. I think it was John Hughes who talked about metrics, about the standards, and which have impact.

Reading the State of Reliability Report, it's obvious we have more and more data on elements of reliability, but the grid is yielding more data all the time with the PMUs and with the analytics that we're capable of with CADs and GADs and so forth. Is there more that we can do in the area of leading indicators of reliability issues with the new data that we have and should we be expanding our data collection? It's always a question of how do you balance using the data to get the lessons from it with protecting it because of the security, but it seems like its more of a data analytics world and I wonder if we're doing everything we can in this area or there's something the Commission should be doing.

MS. HOFFMAN: So I think data provides a great opportunity for improving the operations of the grid,

especially in assess management. I think from my perspective as you look into where some of the leading indicators are goes after, say, some of the data that's been helpful for transformer, looking at predictive failure and assessment management, so I think that's one are of opportunity.

I am concerned about security of the data, but the value of machine learning and being able to get more predictive in nature and looking probabilistic assessment I think really will provide value for the grid.

MR. CAULEY: So I think our ability to collect data from industry and their willingness to provide it to us and to be able to turn it into meaningful results and analysis is really one of the success stories we've had over the last five, six, seven years and I think it will continue. And it's really the foundation to everything we're doing. There are some areas where I believe there's probably going to need more, but we do want to be judicious with the burden and the security issues with having that data.

One thing I know we do need to get is some better clarity and granularity around reporting of security incidents because we have OA417 and we have EOP004 for reporting of incidents, sabotage reporting, and so on, but it's very sparse. And so the question is working with

industry what makes sense to create a sufficient set of data to analyze are the threats getting worse, are things happening more frequently, are the entities getting into our systems, deeper into our systems.

I also believe that we don't have -- NERC has really focused I think this coming year to come up with a better set of security metrics, understand security risks. The idea of, well, no cyber attack is going to cause a blackout. Well, that doesn't mean there won't be one tomorrow, so how do you measure risks, but you need data on the front end to make that happen.

Just to follow up on Pat's comment, I believe getting -- sort of corralling the value of PMU data for metrics is probably on our horizon in terms of understanding behavior system. I think you can see the behavior of the renewable inverters-based resources and distributed energy resources. The granularity of the PMU data is so fine that you'll be able to see the nuances of those measurements and try to get some leading indicators of problems I think through that approach.

CHAIRMAN LA FLEUR: Thank you. I appreciate your comment on burden and I hope we're looking at a future where we pass fewer rules where some busy person in a control room has to fill out one more report because I've been there and I know some times where that priority comes

in versus keeping the lights on and more situations where the actual equipment or the grid is giving us data without human intervention.

I guess let my colleague. Maybe she'll make some of the people I haven't bothered work. Thank you.

COMMISSIONER HONORABLE: Thank you, Cheryl. Good morning everyone and thank you for teeing up a really robust discussion. I'm like, Cheryl, I don't really know where to start, but I will pick up on the Aliso Canyon topic because I think this is an excellent example of the ability that we all have to play a role. And I think Secretary Hoffman mentioned the federal and regional responsibilities, but I also wanted to tee up because Chairman Haque, Chairman Twitty -- I like calling you that Chairman Twitty -- and John Hughes have also touched on this important need to coordinate the federal and state and local level -- that's a nod to folks, the LPPC folks -- but also, making sure we're playing well with our state colleagues and coordinating. I think there's an important role to play.

So while we've been very focused certainly on watching the Aliso Canyon Incident, I want to commend the Taskforce for working diligently on that, certainly, DOE for watching it and NERC's role as well. There's clearly a role for state regulators to play here and I think this Chairman Haque's point as well that states have lead in this area.

And this is an example of the importance of our state colleagues appreciating this issue we got passed last summer, thankfully. But according to the summer assessment, we have to be very cautious going forward, so I wanted to ask the Secretary and any others if they wanted to comment about either Aliso in particular or how we can do a better job of being mindful of our state colleagues' role, but also making room for them to continue leading here was well.

MS. HOFFMAN: So a couple of comments that I'd like to make as I was thinking about this and that there has to be coordination. As the states think about their investment strategy, whether it's generation, whether it's storage, I think there has to be a close coordination with the reliability coordinators in doing a system evaluation so we can stay ahead of the game of what potential investments are required, whether you take the polar vortex, whether take Aliso Canyon, whether you take the Northeast and the gas infrastructure issues.

I think from my perspective the interdependency play is going to be let's take a hard look at the policies, the infrastructures, whether it's battery storage or gas storage. There is some level of storage that is required on the system and think about what are the cost-effective solutions and what really can be optimized to the benefit of

the system. So having that close coordination with the states is absolutely critical.

MR. HAGUE: Well, thank you for the question Commissioner. This question gets more complicated when you start thinking about states that are in organized markets and states that are not. So it creates one grand, circuitous world of confusion when you start thinking about the State Subsidy Tech Conference that you held and it is an extraordinarily challenging issue.

I guess without getting to prescriptive, I have always thought that reliability should be the tie that binds. So in taking my NARUC hat off and putting my Ohio hat on, we have been through the arch of our now famous or infamous PPA cases. There were a tremendous number of policy considerations that were espoused in those cases. I think, though, that what has been missing from the dialogue broadly is the true on sort of reliability concept.

And so because of the market issue, the state that resides in an organized market or your typical cost-of-service state, I don't know that there's a silver bullet to this answer of utilizing whatever comes out of a reliability study to socialize that then across states and have some kind of uniform response, but at the very least, from a policy perspective, again, I do think that we are all on the same page with respect to that particular issue, so I

do think it can be helpful.

And I think that -- look, so I've been doing this now -- this is my fourth year doing this.

COMMISSIONER HONORABLE: Thank you, by the way, for doing it.

MR. HAQUE: Thank you. Again, thank you, I think to that, but thank you for the opportunity. And our state engagement -- the arch of state engagement has dramatically increased over this just four years. Initially, it was just about cost and now we're talking about this concept of base-load resources. We've been talking about that for a few years now and now we're talking about a totally changing even state rubric with all of the grid mode endeavors that you're seeing and how that will interact with the Bulk Power System. So I think you're right and I think we all recognize that. I think reliability is the tie that binds, but because of especially on the bulk side the markets issue it's an extraordinarily challenging issue, but at least on the distributed resources side I think there's some real opportunity there.

COMMISSIONER HONORABLE: Thank you. Anyone else, Chairman Twitty?

MR. TWITTY: Well, Commissioner, I appreciate you particularly pointing out that there is local authority as well. People used to say to me, well, you're not

regulated by anybody. No, you're regulated a local city council or a local board of public utilities or public works or whatever it's called. And I think the point I would make, and it also goes back to the data question a little bit, and that is just a real focus on the coordination of information flow.

Think about if there was an event on the system today you could have three or four or five different agencies requesting information and if you only have to provide it once that's a heck of a lot better than three or four or five. And the same thing about this, just remember that there are local regulators. Steve and I would both we would agree with that, whether it's LPPC or TAPS.

Those folks, again, they're the people, the store or church next Sunday that are going to button-hole you and wonder what in the world happened. And like Mr. O'Neil said once, you know the government that's closest to the people is the best, not to say bad things about FERC or NERC, but it is true.

COMMISSIONER HONORABLE: Thank you.

I wanted to turn now to just acknowledge the fine work of NERC and all of the stakeholders who participated in the supply chain matter. I wanted to say thank you for your effort. I know you worked so hard to get across that line, but I was very pleased to hear the report

that it got through in the second balloting.

And Gerry, I wanted to turn and ask you a couple of questions. One is to also commend -- I teed it up in my opening remarks -- the work of the entire sector on focusing on MISOPS, in particular. And it was really a beautiful thing to watch, to participate with you and your colleagues at the MRC and at the Board level, to engage with regionally, to even sit in, in an RTO meeting. I happened to be in Little Rock at the SPP meeting and heard a very robust discussion about the state of play with regard to MISOPS and what a number of folks across the industry sector were doing to focus on that and we've seen great results.

I also noted in your report that human error, of course, continues to be a challenge, to err is human, and I wanted to ask you what are the lessons that you've learned with your very deliberate approach to tackling MISOPS that you can also employ with human error matters?

MR. CAULEY: That's a great question. I appreciate the feedback. You know I think the story that we're still working on and it's unfolding and really miss operations is really a great example of the ERO should work, which is data points to a recurring theme of harms being done, outages being bigger than it should, load shedding and so on, and we say why is it telling us that. And the volume of data that we can see across North America really I think

is helpful compared to what each company could see because the company's been doing really miss operation analysis for decades, way before we were doing this.

But to be able to see the big picture and to see the pattern at a big level is really helpful. The solutions phrase has really been interesting because we've involved the North American Transmission Forum. Each of the eight regions has their own individual program, so it kind of gets customized and distributed out to get the work done. We're not pulling levers and managing the work.

The interesting piece is there are some entities that have rates high as 19, 18, 20 percent miss operations and some as low as 4 percent. Some of those are for reasonable, physical reasons why because the system design is different and different geographic areas, but it tells us that we can focus on particular regions or we can focus on particular entities and drive the performance to continue to be a lot better.

I think we can repeat that in the human error field with one concern, so that the solutions in relay miss operation space are very technical, so there's a series of loose connections, polarity reversed, the communications are not correct to coordinate between two relays that need to talk to each other. So the solution space in relays tend to be technical, mechanical, objective things you can do. And

once you fix them, they're kind of fixed. But if you can imagine now where I'm going with this, it's going to be a lot more different things can happen. You don't just fix one thing one time, so we're working, once again, with the Forum. We've done a joint workshop with them. We're doing peer reviews of best practices in human performance, but it's much more of a morphs transition. It's not fix one thing at a time. It's going to be building awareness, building best practices, building controls around that and I think we'll see a similar trend in human performance. It has gotten better in terms of impacts and I think we'll start seeing a sort of level of excellence in human performance in terms of error rates we'll be seeing in the coming years.

COMMISSIONER HONORABLE: Thank you. And I want to thank you and your colleagues and all stakeholders in advance because we know it's something that will occur, but I appreciate the focus on it because I'm certain there are certain areas that are common -- you know common human errors that can be focused on and I appreciate that you have already seen that and seen ways to improve it because the system is benefitting from it.

I wanted to touch on the Blue Cut wildfire incident because you mentioned the tripping of the two 500kv lines in the fire area and the loss of more than a thousand

megawatts across multiple areas and I wanted to ask you what did you learn from that and what can we employ going forward to be responsive to a situation such as that. And I'll also give Cheryl an opportunity if I didn't quite ask her question to jump in.

MR. CAULEY: I think we learned at different levels. You know at the highest level in terms of ERO role, once again, going back to the data having data and having -- this was not really a reportable event. It didn't actually make the news.

COMMISSIONER HONORABLE: And if I could say, that's why I was particularly interested in it, the fact that it wasn't a reportable incident.

MR. CAULEY: But we saw a series of frequency anomalies that day and we looked at why did that happen, but we had the data and we were able to work with Cal ISO and Southern Cal ISO and others to like let's investigate this even though it doesn't hit the criteria to require an investigation, but it's really interesting, and so we were able to do that, so one lesson is keep doing this.

I think with the introduction of DERs and renewables and inverters and new technology keep looking for anomalies that we don't understand why they're happening, keep digging.

I think we learned, as I mentioned, that the

standards talk about ride-through for generation. Once we investigated this event with the vendors, their understanding of ride-through had nothing to do with our understanding of ride-through. Our understanding of ride-through is you keep producing megawatts because if something's happening on the system around you, you don't want to like drop your production and increase through a cascade into further frequency. They thought ride-through was just shut off the power, but hang on there so they're connected, but they're not actually producing anything.

And we also learned that introduction of time horizons, and this is not just in wind and solar inverters, but this is in distributed energy resources and new relays that are coming in that a lot of this equipment is operating in microseconds and they're deciding and acting and doing things before the old, clunky, moving things have time to move or do anything, so that creates a whole new field of reliability concerns is how do we coordinate. The solution in this case is that the manufacturers are telling us, well, we can slow that down. We just didn't know you needed that, so we can put a five cycle delay or a second delay on something and let the system do what it's supposed to do before we decide what to do.

So I think there's a lot to learn and I think it's a field that's going to be at the forefront of

reliability for a long time.

CHAIRMAN LA FLEUR: I guess my question, and it was really a question that was provided by David Ortiz. I don't think I'm smart enough to think it. Is this an issue that's endemic to inverters generally that we need to watch for other places or was it just kind of growing pains on the assumptions and calculation frequency? So I mean how much do you think we need to look across to other situations versus just something that would sit there.

MR. CAULEY: Well, I think this is everywhere. This is basically, as we were thinking our strategy on how do we deal with new technologies, one thing we've realized is there's a whole lot of players now involved installing equipment on the system who probably many of them still don't know who NERC is, but certainly, they didn't know who NERC was a year or two ago. But they're putting equipment on a system at high volumes of resources and so they don't understand what the terminology means. They don't understand how we measure frequency and voltage and what the words in the standards mean because we do have a clear blueprint in the standards for how generators should behave when they're connected to the system.

Now we're miscommunicating because their understanding is at a level of electronics and the speed of their systems and this is a different level. So I think

it's widespread.

One of the things I wanted to do is make sure we get this quick enough that we don't get into regrettable situations in terms of installation of new facilities. And we're still investigating, but the vendors have told us that 40 percent of the inverters that were involved in the Blue Cut incident cannot be corrected for the voltage problem. So that means they're producers. They can produce megawatts. They can be there. The can be planned for, but if there's a disturbance you have to assume that 40 percent of that generation will leave.

So what we want to do is get the work done urgently enough that we don't have any more facilities installed that don't have the capability to operate and it's expensive to replace them once they're in.

CHAIRMAN LA FLEUR: Needless to say, when I've talked to solar industry groups and wind industry groups, I frequently urge them to get more involved with NERC, so I'll use the bully pulpit here. It's really essential.

COMMISSIONER HONORABLE: I, too, think Gerry your comments speak to not only flexibility, but inoperability and just reminds me of when I was chairman of Arkansas Public Service Commission and we would have a mayor who was gung-ho about putting a wind tower up, but had no clue of -- some vendor came and said, no, put the wind power

up and then go to the Commission. You know he didn't know he needed to come to the Commission and the fact that he didn't come first caused a whole world of problems for him.

And to your point, our ability to master how we're working with integrating these inverters in such an credibly wonderful time with greater amounts of renewables, but our ability to harness that in a way that still gives us -- I think Pat spoke to being nimble and flexible -- still allowing us to do that. So thank you. I wanted to ask your lessons learned.

I wanted to turn to both, Charles King and Mr. Wright, because you both, in your comments, teed up a discussion I wanted to have. One is I too want to commend the industry broadly, and when I say "industry," all stakeholders, but yes, industry meaning EEI as well for your leadership in the ways in which you continue to work.

I agree with you that, yes, we need standards, but that there are number of ways in which industry, collectively, the sector, is working in ways -- I love the way you said it -- to supplement this important work. So it's a great time for us to reflect upon now 10 years of mandatory reliability standards, but it's great to talk about the ESCC work, the work happening at the ISAC with the ISAC effort, with fusion centers, with all of the ways in which we're working together. And I'm very pleased that

you mentioned mutual assistance, the spare transformer efforts. So I wanted to take this moment to thank you and your colleagues at EEI for your leadership there.

Mr. Wright, you raised an interesting point about the fact that, in your opinion -- and I wanted to ask you to talk more about this. You think that we may need to create more incentive or did I write "rewards" or did you say "rewards" for compliance? This is an interesting discussion in my mind because I have a 16-year-old and she gets good grades, but I think she could get better grade. So do I reward her for -- you know where I'm headed with this -- for getting the grades she should be getting anyway.

MR. WRIGHT: I have a 17-year-old son, so I'm right with you on this one.

COMMISSIONER HONORABLE: So we're speaking the same language. I want to ask you to elaborate on that because I think even in the context of our work here at FERC we have heard some stakeholders saying this is the work we should be doing. This is our job. But I want you to talk more about using this carrot approach versus the stick approach. I think for us in the U.S., I think we've seen it work particularly well, so I wanted to invite you to talk more about that.

MR. WRIGHT: Well, I think this is a little bit of the conversation we were having earlier too. I want to

spend some more time with Gerry because I heard him say that there is a way to work with the regions that maybe has not been fully exercised yet and I'd like to understand that better because I think one of the things that has happened is the whole commitment to the RAI Program has caused utilities to go down this path of doing really elaborate inherent risk assessment and internal controls evaluations work. And I just say from my experience that has been really good work. We've learned a lot of things that we didn't know about the way our systems operate.

We've learned about the way our system impacts the Bulk-Electric System that we didn't know and probably should've known, so there's been some really valuable things that have happened there. There should be an opportunity as well to be able to learn there are places on our system that have a big impact and we need to really be focused and there places on our system that don't have a big impact how can address that in terms of trying to wring some efficiencies out the system. I think that's the challenge that we face.

COMMISSIONER HONORABLE: And really take a risk-based approach.

MR. WRIGHT: That's right. So that had been, at least from my understanding when we first started down this path three, four years, were I said we were going to go out and we were going to learn a bunch about where it is that

individual systems and eve facilities within systems were really critical to the system and were they were not and that we would be able to advance our protection of the system through that knowledge that we would gain.

And so we're now to that point where we've gained a lot of knowledge. Now the question is how are we going to exercise that knowledge to be able to take advantage of it. And again, we're spending a lot of money on this. I think it's a good thing because we're improving reliability, but if we can find efficiencies, we should go find them and try to get them.

COMMISSIONER HONORABLE: Thank you. Any others want to comment on that point?

I, too, appreciate Mr. Wright that you mentioned opportunity at the regional level.

To Chairman Hague's point, I think that could open up another level of complexity. I think we continue to have discussions about the best regional approaches and ways to get regional efficiency in the context of enforcing mandatory reliability standards, but also harnessing greater efficiencies in our day-to-day reliability work. So thank you for mentioning that and I look forward to greater discussion about the best ways to do that going forward. And thank you all for appearing here today.

MR. BARDEE: Thank you, Commissioner. I think

staff we'll keep our questions to a minimum so that we don't get too far off schedule. I'll just ask one at this point and it's actually something that you might be able to address, Pat. Others are welcome to also, but it goes to the supply chain issue.

As you know, we required NERC to develop a standard. There's a standard in the process. It just passed its second ballot. Presumably, it'll come to us sometime later this year. And if we ever a quorum again, we'll do something with it, but at best, that is a solution that deals with a small part of a very big supply chain. It may reduce the risk for the entities subject to it that apply it, but the supply chain itself involve so many sectors and so many other aspects that are far beyond our role and I was wondering if there are efforts or things that DUE in conjunction with perhaps other parts of the government would be able to or is considering doing that could address parts that we can't.

MS. HOFFMAN: So thank you. That's a really important question and it's quite a complicated subject, as you talked about supply chain encompasses more of the subcomponents and parts and pieces than what was directly reflected upon in the standard. So some of the things that the industry should think about is trust in manufacturing and looking into assessment of the manufacturing process.

One of the things that the Department's looking at and considering is how do we further do testing and system testing of supply chain components so that we actually can have feedback to the industry from a risk assessment point of view. At the end of the day, it's going to have to be a collaborative process where industry understands the risks that are being posed by the supply chain components and their subcomponents, but also it has to be some disclosure of where some of those vulnerabilities may be. So we're going to look at some system testing, but we're also thinking about how do we learn some lessons from DoD from a trust in manufacturing point of view.

MR. HEGERLE: So let's try to tie together several things. I liked Gerry statement on fearlessly focusing on preventing the next outage. And Acting Chairman LaFleur mentioned data and metrics and others of you of the panelists mentioned that as well and Commissioner Honorable mentioned the learning that we could get from the MISOPS as applied to human error.

I was wondering about how well we can look at the interdependencies of these various data pieces to do that prevention in that when we look at averages we don't end up necessarily seeing the picture in a specific region or with specific entities that are close together and many of the outages that we've seen like the one five years ago

out West was one where one small mistake preventable was made by one entity, another was set up differently and a third and we have a problem. Is there a way? Can we, do we look at the interdependencies of those various pieces at a more macro -- not an individual entity, but a smaller, maybe a BA-area way of thinking about that or identifying those risks so that we can prevent, as Gerry was suggesting, those bigger events?

MR. CAULEY: Well, if I could call up Dr. James Merlow from the audience here, he could probably help me answer this better, but we are not focused simply on using averages or broad pictures, but we have some very good PhDs and statisticians on our staff that are looking for the patterns that are hidden in the noise and some of it I would call it sort of transactional or sort event drive. So you look for an event and you try to figure everything out and others are just sort a broad collection of data over time.

I think the one opportunity we could probably explore a little bit more is the interdependencies between the datasets. Now we do that to some extent now like if there's an event we're looking at the transmission performance through the TAPS database and we're looking at the generator performance through the gas database and saying well why did they all combine to leave. So we are doing some cross-dependency, but I think the error you're

talking about I think is a new opportunity maybe. Even when there's no event and it's a sort of a blue sky day, are there any correlations between data and across the databases. I think that's an interesting question. We'll talk about it when we get home.

MS. HOFFMAN: If I may add one thing. I think the value of the PMU data is a dataset that's consistent across the whole industry that provides a platform where grid operators can look at consistent tools and actually be able to do forensics and analysis and asset management. So moving forward, we need to have a similar set of platforms of data, whether it's sensor-based data, the distribution system that the industry writ large can build upon for visibility and really speed up some of the understandings of what's happening and that has to be paired appropriately with the data that's feed into modeling and analysis of the system

MR. BARDEE: So with that, I think we'll conclude our first panel. I'd like to thank all of you for your time today and we really appreciate it.

MR. WRIGHT: Mr. Bardee, can I make just one quick comment, if I could? I'd appreciate it.

I did participate in the first one of these conferences way back in -- I think it was 2010. And there was a lot of tension in the industry at that point and there

was one of the reasons for this conference. And I just want to say back I think at the second conference I made a recommendation that this be formalized and happen more frequently and I want to say right now that that was unnecessary. And the reason it as unnecessary is because of the way folks have chosen to participate in processes since then. So Gerry has run his organization in a very transparent way that made it not necessary to do this.

The FERC staff has been much more open, I think, in terms of engaging with the industry and the Commissioners have gone to the MRC meetings. So for really good reasons collaboration has occurred and I just want to say that has made this law work a lot better and I appreciate it.

MR. BARDEE: Thank you. Thanks again.

So if our next set of panelists could please come to the table.

Alright, we're going to start our second panel now.

COMMISSIONER HONORABLE: Mr. Bardee, if you don't mind, I'm going to raise my voice a little bit. Ladies and gentlemen, I love that you're enjoying this so much, but we are going to proceed to our next panel. Thank you so much for your attention.

MR. BARDEE: That's why she's a Commissioner and I'm just a staffer. So let's start our second panel here

with speakers from other parts of the world, not the United States and it's an opportunity for us to hear what's happening in other countries, North America and Europe, and to learn what we can that may help us and share our experiences. So I will start by introducing Mr. Brian Hewson from the Ontario Energy Board.

STATEMENT OF MR. BRIAN HEWSON

MR. HEWSON: Acting Chair LaFleur, Commissioner Honorable, staff, and my fellow panelists, good morning and thank you for the opportunity to come and speak today. My name is Brian Hewson. I am the Vice President of Consumer Protection and Industry Performance at the Ontario Energy Board, which is the gas and electric regulator in the province of Ontario in Canada.

And while I will touch briefly on some matters of all of Canada, my remarks will generally focus largely on Ontario because that is where I'm most knowledgeable and most experienced. And I think the experience that we've had in Ontario will touch very closely on a number of the questions that were asked in your agenda.

Canada and the U.S. are a highly integrated electricity network system. As you will know I'm sure, there are 34 interconnections between U.S. states and Canada. There's also 33 major inter-prevental connections, which makes inter-ties a very important part of the

operation of our grid in Ontario and a very important part of the operation any considerations of the OEB.

As you know, unlike FERC, in Canada each of the provinces and territories are responsible for reliability oversight of the transmission network. You know following the 2003 blackout, the federal and provincial ministers of energy got together and decided that there should be a close cooperation and coordination across the country and they've established a working group, which we are a fully active member of, that coordinates and discusses both activities in relation to NERC and activities across the country in terms of coordination and ensuring reliability.

Each Canadian jurisdiction has implemented its own approach to ensuring that reliability of the local electricity system is taken care of. Each enforces NERC compliance through a variety of models. In Ontario, I'll speak to specifically, our independent electricity system operator is the designated entity that's in charge of ensuring reliability of the system and monitors and enforces the reliability standards enforced by NERC with the Ontario Energy Board as its backdoor or backstop, I should say. We are there to make sure that if someone needs to have further sanctions against them, we are in the position to do that.

You know your questions really focused us on the issue of renewable and distributed generator and how Canada,

and in my case, Ontario is managing the evolutionary change. What I can tell you is that the provinces of Canada are heavily involved in renewable energy. As you will have seen in my notes that I've provided, roughly, two-thirds of the electricity that is provided in Canada is produced through renewable sources. And that includes the provinces of Newfoundland, Quebec, BC, Manitoba, and Yukon where they rely on almost 95 percent of their electricity is produced through hydroelectric facilities.

Ontario -- now I'm going to focus a little more closely on Ontario -- has gone through a significant supply change over the last 10 years. By 2025, our IESO is forecasting we will have renewable resources connected at both the transmission distribution level that nearly make up 50 percent of installed generation. The bulk of the rest of our generation is nuclear and we are in the process of a major refurbishment of all of our existing nuclear units to be able to continue their operation.

We did change and increased the renewables as part of a government desire to eliminate coal as part of the Ontario supply mix. While we were eliminating coal, we recognized that we were bring on intermittent renewables and that that required changes to our market rules to make sure that intermittents were playing their proper role within the IESO grid and IESO markets as well as investments in

upgrades to both transmission systems and distribution systems.

At this point much of Ontario is looking at approximately by the end of this year having over 3600 megawatts of distributed generation. That compares to the mid-2000 when we had under 100 megawatts of generation that was connected to the distributors. That distributed generation is causing many changes in our system. We have facilitated the change through rules to require nondiscriminatory access by distributed generation. We've imposed contract requirements that ensure that connection processes are timely, but respect reliability and security requirements. We've also implemented changes to rules to facility good public policy.

On the gas side, I did hear mentioned we have recognized the importance because of the increase in gas generation to be assured that there is good coordination, so the IESO has been required to develop a coordination taskforce with the gas distributors and gas generators. As well, they have implemented a new grid, LDC, Local Distribution Coordination, Committee to ensure that there is greater task connection and data sharing across the two entities.

They've also focused on frequency regulation, voltage control, and flexibility increases.

In closing, I'd like to say that the provinces and territories in Canada will maintain our collective and collaborative efforts to ensure that successful outcomes continue to be achieved as the supply situation changes and evolves. As the first jurisdiction in North America to implement mandatory NERC standards, Ontario plans to continue to play a key and leading role in that collaborative effort.

I thank the Commission and look forward to any questions.

MR. BARDEE: Thank you, Mr. Hewson. Next, we have Commissioner Madrigal from CRE in Mexico.

STATEMENT OF COMMISSIONER MARCELION MADRIGAL

COMMISSIONER MADRIGAL: Thank you very much, Chairman LaFleur, Commissioner Honorable, colleagues, we think a lot of your invitation to speak on behalf of the Regulatory Commission in Mexico. We believe sharing experiences is very important. WE have learned a lot from our neighbors in the process of implementing this tremendous energy reform and I will speak in my remarks about the reliability issues with regard to integration of renewable, distributed generation and some of the issues that we are seeing in the gas markets, so I really thank you for the opportunity to be here.

Most of my comments will be, of course, personal

comments. When there are Commission decisions, I will clearly state those aspects. So with perfect ongoing energy reform in Mexico, renewables will increase up to 35 percent by 2024. Right now clean energy sources in Mexico are about 20 percent. In our legislation, clean also means large hydro, including nuclear. We have a large nuclear power station. So out of those roughly 40 percent of -- renewable resources, mainly, wind and solar, but with the recent success of the energy options, we may reach 10 percent of whatever renewable resources just in a question of one or two years.

Why? Because we have contracted roughly 6 g-watts of new capacity to be added in the next two years, mainly, solar because of the attractive prices we are getting in the market. So what we have been contracted recently is more than what the system has added in the past eight to ten years. So we are going to see a very rapid increase of valuable resources in the next two to three years, reaching up to 10 percent of valuable resources.

In the distributed generation, solar is growing exponentially. Roughly, 40 years ago, we had zero installations at the distributed level, now we have 29,000 installations. Roughly, they make up for 250 megawatts and the size of the installations are growing from an average 5 kilowatt to 10 kilowatt. The Commission has issued rules to

continue with distributed generation. We have three streams -- net-metering, net-building, and wholesale of distributed generation to the spot market now that it is facilitated with the energy reform. So we continue using net-metering as a way to facilitate consumers engagement with the market. Of course, those mechanisms will evolve. The new rules have a sunset clause. We will review those, but we believe this is an efficient way to make consumers ready to engage in these activities.

The grid code level we're incorporating some smart and better features into our distributed generation rules so our control center in Mexico is gaining expediency on managing renewables. As part of the new market rules, all renewable suppliers have to provide forecast to the -- . This is the control center. They improve that forecast. And in the last issue transmission investment plans in assay is really looking ahead on what investments are required for the suns that is more investment in solar power. So proactive planning to make sure transmission reaches those areas in a reliable way.

As part of the reform, we create in Mexico it's like FERC, NERC, and the state regulated altogether, so we have the responsibility to look after wholesale, retail rates, reliability at the federal level, so we issued the first independently release grid code, which is more the

reliability standards as a whole, include planning, operations, and interconnection requirements. We are using the expedience worldwide in terms of making sure we have technologies that cooperate with the grid. We are in the process of preparing the first annual, independently issued reliability report and we will see what happens and what revisions in the first version of that reliability report.

On the gas side, as you know, natural gas is very important for us. We rely a lot of imports from gas from the U.S. as 55 percent of our gas supply comes from the U.S. and makes for probably 40 percent of our electricity mix. We're also in the process of creating a gas market in Mexico. At the Commission last week we basically freed the previously regulated wholesale price of gas. We're in the process of building a market and in that process there is also an independent system operator of the gas market recently created with the energy reform. Its name is Senegas. And Senegas now that our market is evolving in gas it is also in the process of writing the first grid code for operating the gas infrastructure of the country. There we have jurisdiction. We approve the rules for the gas system operator, so we are in the process with technical groups to write that code.

Of course, any reliability issues in the gas sector has big implication for the power grid in Mexico and

in the expansion plans of the power sector. The Commission has issued comments that this interaction should be looked after more carefully from the planning perspective, so we have been able to manage issues with gas supply mainly through demand production programs and we continue to work in that.

Now looking ahead, the Ministry of Energy, which is the policymaker in Mexico, is in the process of drafting a gas security supply policy, looking at possibly storage quotas. We don't have a policy yet. A policy is under consultation for the fuels market and we already have a policy on the security of supply for the power grid.

So that was basically my general comments and I look forward for a deeper discussion. Thank you.

MR. BARDEE: Thank you, Commission. And finally, we have Klaus Dieter Borchardt, Director for Energy at the European Commission.

STATEMENT OF MR. KLAUS DIETER BORCHARDT

MR. BORCHARDT: Thank you very much, Mike, Acting Chairman LaFleur, Commissioner Honorable.

First of all, I'm very happy to be here again and that FERC has invited me again to this conference here. It's a real honor for me to be allowed to present the European view in this panel.

As you all might know that the European energy

system is already in the middle of profound change. All had started about 20 years where we had broken up the structures of the more than nationalized energy markets by unbundling the by then integrated, vertically integrated companies and unbundling them from production and supply and transmission. That was the first important step.

The second step in these changes were the creation and the development of network codes and guidelines, a bit similar of what I've just heard here from my Mexican colleague. This work we have nine network codes and guidelines. This work has been finished recently in March this year with balancing code in electricity. And now we are just entering in the next phase and this phase has very much to do with what I call flexibility.

Why is that so? The European system, of course, is based on a new climate policy to which the European Union is heavily committed. We have initially started by giving ourselves legally-binding targets. They are running of 2020 was minus 20 percent CO2 emissions, 20 percent share of renewables, and 20 percent energy efficiency. And now within COP21 and Paris Agreement Complex, we have globalize new commitments time horizon 2030, minus 40 percent CO2 emissions, at least 27 percent share of renewables in the system, and 30 percent energy efficiency.

And when you look at, at least 27 percent, this

is necessary in order to make it up to the 40 percent CO2 emissions because 60 percent of the emissions are coming from the energy system. And 27 percent means not less than 50 percent of the whole electricity consumption use, have to come from renewables and here intermittent renewables, solar and onshore winds, but offshore winds coming very strongly.

So this, of course, creates huge challenges for our energy markets, but not only the markets, as I've said, for us the drivers for reaching our climate goals are energy efficiency, so therefore we have proposed a profound reform here as well, and renewables. And this, of course, now has to relate to the market. And what we can see is that the market, as it stands now, is not up to the challenges.

We have not enough flexibility in the market, neither on the generation side, nor on the demand side and this is, of course, of paramount importance because we still firmly believe that a well-functioning market is the most cost efficient way to deliver electricity to the consumers. So therefore we have put forward as a Commission a very comprehensive package, not less than eight legal acts comprising in a clean energy for all European package and it's free of these concerning the market design of the electricity market.

And I would like just to focus on the four building blocks of this market design, part of this package.

The first building block are the consumers and here we are trying to put the consumers into the center of our energy system and trying to make them participate in the development of our energy system.

And I will only highlight two concrete measures here. The first is that we give them an unconditioned right, all consumers, individually or collectively, in energy communities to produce, to store, and to sell energy. The second is the demand side response. Here we foresee two different ways. One is price driven. Here we provide the consumers with dynamic pricing systems and smart meters so that they can adapt a consumption to the price situation and the other is incentive-based. Here we are creating a very robust legal framework for aggregators so that they can enter into the market and do this demand side management.

On the wholesale market, of course, it is the integration of the intermittent renewables that we have and here it's very clear that we are moving away from base-load capacity to flexibility. Our intermittent renewables are not reconcilable with purely base-load capacity approach. How do we do that? First, we have to make the market fit for the renewables and that means in the first place we have to reform our balancing markets. We need much, much more balancing reserves and we need, of course, services at very short notice from generators and from the demand side

response in order to keep the system balanced in real time.

Here we are moving the balancing from the national to the regional level, so the calculation and also the procurement will not be done within the realms of the member state, but in the region. We are also finalizing our work on the short-term markets, which will become even more important in the future. So intra-day and day-ahead market coupling is about to be finalized.

Another issue is the pricing system. We are proposing that the price setting should only be done according to the market signals, nothing else. So that means that the old price caps and the regulated prices that you see in a number of systems in different members states -- 17 members states still have regulated prices -- have to be abolished and we've proposed that. We also want to allow prices to rise to the value of lost load in order to also reflect scarcity, so scarcity pricing has to come.

Another issue you know in Europe we are following the sonar pricing approach. The configuration of price zones is also an issue. The problem we have today is that the price zones are not designed where the congestion is, but under political considerations and it's political borders that are prevailing over the economic and technical ones and that we are changing as well.

We are introducing capacity mechanisms, but only

as a last resort instrument, capacity mechanisms that have to be proven its necessity at regional levels. So the adequacy assessment has to be done at regional level, not any more at national level. It has to be cross-border open so that can also companies from -- and other member states can participate in that end. Here we have introduced as well an emission performance standard, 550 grams CO2 per kilowatt hours, which will kick out or not allow in coal-fire power plants and some even gas-powered power plants. That's what we are doing on the market side.

On the renewable side, here we are bringing all of the renewable producers under the same obligations as any other generators, so that means balancing responsibilities, no priority dispatch any more. Another very important is because if you have more renewables you have decarbonized generation and you have closed integration. What does that mean for the interoperability? That means that we'll have much, much more interrelated system operations.

And in order to cope with that, we want to create the so-called regional operational centers. Here we have an organized cooperation between the respective TSOs in the regions and this ROX as we call them, they will at regional level do the sizing of the balancing reserves. They will do the capacity calculation. They will care about security and safety issues and they will also do their

generation adequacy.

The third building block is infrastructure. And here I can say that we have a well-working planning system in place with a 10-year network development plan, with a project of common interest, and to connect a newer facility bridging financing gaps, so this is all working well. But what we need more is very strong cooperation between DSOs and TSOs because in Europe the renewables to 60 to 90 percent are going directly into the distribution grid and they cannot cope with that alone, so there has to be very, very close planning and managing cooperation between DSOs and TSOs and we are putting the respective rules in place by creating a platform on which DSOs and TSOs have to carry out specific tasks.

And then, finally, digitalization as the building block. Here I have to say that our proposal currently in discussions in the Parliament and in the Council of Ministers has only some elements of digitalization like smart grids and smart meters innovation, how to bring more innovation into the energy system. But I think in future, and this is maybe a new challenge, more has to be done. We have to think about to use block chain here in order to make possible to be peer selling. I have heard in the previous discussion. I think you, Acting LaFleur, have mentioned that we need in real time information from

the grid, so you could also use this new databases to give us automatically without intervention of human beings this information. This is absolutely important. Also, the automation of the houses so what happens behind the meter will be an issue. We have not addressed it yet.

And last, but not least, also cybersecurity. My colleagues have mentioned gas. Gas is not part of this package. We are concentrating on the electricity side. We have a well-functioning gas market. Gas in this new system, in my view, will stay as a backup. We will go out of coal. Some member states will continue with nuclear, traditionally. We might have one member state staying in coal. That's forgiven, but mainly there is gas to stay as a backup.

So all-in-all, I must say that we have now a 1,000-page legal work on the legislators' table. We hope that we can get it through because without the changes that I have just mentioned briefly it will not be possible to live up to our commitments. Thank you very much.

MR. BARDEE: Thank you, Klaus. Commissioner Honorable, questions?

COMMISSIONER HONORABLE: Thank you, Mike. And I want to welcome our guests here and please know we are delighted to have you as part of our annual reliability tech conference. For our European colleagues, thank you Dr.

Dieter-Borchardt for continuing to grace us with your presence and we've learned so much from one another. And we were very pleased to host the European Commission here at FERC. I believe it was last year and we executed an MOU and we are honored to work with you.

And to our North American friends, I want to welcome you back as well, and particularly, you Commissioner Madrigal. And we have enjoyed cheering on our colleagues in Mexico and we talked about this quite a bit in our last annual reliability tech conference. And in fact, we moved this session up because we don't want you to be the end of the day because it's important, our work together. We've really been very pleased with all of the work occurring in Mexico with your ambitious energy reform, with standing up the grid code. We cheered you own when you got through your auctions and now to watch as you are standing up your gas grid code and market. We know that we are interconnected.

And I say the same thing to our Canadian colleague. I mentioned to Mr. Hewson before we started that I was just in Vancouver at the CAMPUT meeting. We were there together. And we are also interconnected in our work, both on the electric and gas side. And I'm particularly interested in the work in Canada in developing your carbon pricing scheme. I developed an international mentoring

program for women in the regulatory sector. And Rachel Levine is, or was, my mentee, so I learned a great deal, I know you know her, and learned a great deal from you all and I wish you well with that effort.

In the interest of time because I had a previously scheduled commitment, I will ask you one question and Chairman LaFleur is kind enough to ask my other question.

So I wanted to focus on our North American colleagues first. You both have talked about the dynamic shift in the energy mix and in particular the role that gas is playing. I wanted to ask you to talk with us about your gas/electric coordination efforts.

In particular, Mr. Hewson, I know you mentioned the IESO Taskforce and the grid LDC Coordinating Committee. Will you talk a little bit more about that? What is the mission or goal of each? How do they work together? And then I wanted to ask the same thing of the Commissioner? Thank you.

MR. HEWSON: Yes, thank you for the question. So first touching on the Gas and Electricity Integration Taskforce, back in about 2005 or so, as we saw the increase in natural gas as part of the electricity infrastructure, we actually held a proceeding to look at how to better ensure there was integration between electricity and the natural

gas systems.

Out of that, we focused on -- our rule was to focus on issues around transportation, gas rules, and storage gas rules and we implemented an actual first-of-kind in Canada what's called the Storage Access Rule, which defined particular considerations around more intermittent or required services like gas.

While we were doing that, our IESO actually decided that it should build a stronger relationship with the gas distributors in Ontario, who operate all of the high-pressure transmission system and deliver gas to all of the different gas generators, so they've had that Taskforce for probably about seven or eight years and it meets on a regular basis. And what they do is they share information between the distributors and the IESO to ensure that IESO is building in any planning issues related to the gas distribution system, upgrades to the transmission system and consideration in terms of its forecast for how the gas generators are going to be used.

As we've moved off coal, brought in more renewables, the gas generation system has obviously taken on a much greater role in terms of both reliability and meeting peak demand and so there's been a lot more work there. The LEC grid coordination work is something that the IESO started just a few months -- well, maybe not even a year

ago. After having conducted a few pilots with different utilities, learning about distributed generation and other distributed resources like storage were impacting on the distributor in flowing up into the system, they decided that they should actually form a union with the -- we have 70 distributors in Ontario, some very small, a few somewhat large, but they organized this so that they could start building a dataset and better mechanism for sharing information back and forth.

They have imposed requirements on large renewables that are embedded distributors to actually start providing reporting now and have done so for some time, but they're now looking at the next level down below 500kwu. They're looking to get deeper and deeper into the system.

COMMISSIONER MADRIGAL: Thanks Commissioner. Yes, in Mexico, the growing investments in the gas infrastructure are driven by the power utility, so from the beginning there is some sort of coordination.

Now formally, at the planning level, we, at the Commission, issue recommendations of both the transmission, the power electricity plan and the gas pipeline plant since we also approve the rates for the nation electricity grid and the national pipeline, so I see the Commission as being the facilitator of making sure the plants are efficient for both systems together. So we have issued comments of making

sure gas and electricity coordination is conducted well, especially in some areas where there may be competition between gas pipelines and electricity infrastructure. We have the ability to do that from the Commission.

At the operational level, there are actually already some rules to manage gas alerts. You know in Mexico demand still grows 3 to 4 percent and I think this year it's going to be a record hit of almost 5 percent, so our issues with gas were alerts. We consume all the gas we get and four years ago we had some alerts on gas availability or because of pipeline issues, so the power utility was able to manage those alerts by voluntarily demand reductions.

Now moving to a market, those rules to manage alerts have to be written in a way that are transparent to everyone, so as part of the market operational rules because we still have the issue of gas availability as some point we may have, so we wrote those rules to manage gas alerts.

Going forward, as I said, we're working with the gas system operator now to provide the gas operating rules or the grid code for gas system. So I think our ability to see what is happening in both sectors comes from the fact that both systems are a federal issue in Mexico. We see absolutely everything -- gas, electricity and we have the authority to approve rates and to comment on the investment plan. So the systems are growing and interconnected. There

are many things to be done still, but I think it's systems that basically have grown side-by-side and we're just hoping to continue like that.

Gas is very important for us, although we don't have a lot of availability issues, in the areas where we have lots of wind power, hydro, and gas combined cycle plants have been key to respond to some variation issues locally because of some transmission congestion, so we see that gas will continue to be a clean, cheap fuel for the transition, but we're actually phasing out the companies, some fossil fuel burning because of gas prices. So it happens to be a win/win. Gas will help with reliability and is helping lowering electricity prices.

COMMISSIONER HONORABLE: Thank you both and we'll continue to work well together; I'm certain of that. And please know that you're all welcome here any time. Thank you.

CHAIRMAN LA FLEUR: Thank you Collette. I'm going to start by asking Dr. Dieter-Borchardt one of Collette's questions, but I'll make it the first person plural, I think.

We, too, think that we need a greater flexibility in our markets to respond to the dynamic shift in energy production and consumption. And her question was what lessons learned can the European Commission share with

us as you've focused on this issue of managing the dynamic supply and consumption.

And I'm particularly interested -- this me speaking now -- in doing it with very little reliance on natural gas, which seems to be the go-to fuel to balance variable solar generation here in the United States in many places. So I'm very interested in your experience there, and then I'll ask your colleagues if they'd like to chime in anything.

DR. DIETER-BORCHARDT: I think to have the full answer you'll have invite me again once we are there because we are now really in the transition towards the system. For the moment, we have a clear base-load driven system that does not differ so much.

We have the particularity in Europe that each member state can decide on its own energy mix, which makes our life, when you have to bring all these together at the European, not easier.

CHAIRMAN LA FLEUR: We have much the same in many parts of the United States.

DR. DIETER-BORCHARDT: So then you know what I'm talking about. But anyway, what we are seeing is clearly that flexibility on the generation side what will that mean. I mean we will clearly go in Europe for very, very high share of renewables and mainly intermittent renewables in

future. It will be, as I said, solar, onshore, and more and more coming offshore wind and then you have some niche products. I'm not talking about that.

So that will be the mainstream of our generation. And in future it will be, in my view, backed up mainly by very, very flexible power plant, CCGTs. There you are coming back to gas and here you have the combination coming back to the first question. It is not in Europe without criticism because our problem with natural gas is that we are dependent on imports, more than 50 percent we have to import and our suppliers -- not all our suppliers are the most suitable one.

I would say for business that is not policy driven or even geopolitically driven, and I think you know what I mean, but in my view, the role, if I come back to the question before how we combine electricity and gas is more that we try to develop technologies that are economically viable to transform power to gas and using this. That's one of the fields where we come together.

On the pure flexibility, as I said, generation it will be highly intermittent renewables backed up with, in my view, nuclear and this flexible gas-fire power plant. If there's other power plants that have the same flexibility and we had discussions recently in China. The Chinese they are working on very flexible coal-fired power plants where

they can even meet our emission performance standard, they say. Then of course, that could be an option for those countries that are staying within.

On the other side, on the demand side, the flexibility here we see in Europe huge potential. If you look at it, currently, we are only taking in 21 gigawatt on demand side management. If we implement our proposals on demand side management price-based and incentive-based, we can go in 2030 to 160 gigawatt, so there is a huge potential also on that side really to bring this flexibility to the market.

CHAIRMAN LA FLEUR: I'd like to ask Mr. Hewson and Commissioner Madrigal if you'd like to chime in anything on that question or I'll move on.

COMMISSIONER MADRIGAL: What I think has been interesting for us is the discussion of when and what solutions do you need now for your level of penetration. What we're seeing in Mexico is that we could reach 10 percent of variables so quickly, like in one to two years, that we need to know what we need to do faster than, for example, -- in Europe, so not all countries can reach higher levels of penetration faster, so we need to implement the solutions faster. On that we're just learning from experience and learning from you, from Europe. And looking ahead, we're actually collaborating with -- to perform a

North American integration study to see what would be the solution for higher levels of penetration.

We do have some issues in an isolated area of the country -- very small, 200 megawatt system that is insulation. We set up a limit in that region and the limit was reached almost at the moment the rule was issued because it's so attractive solar power in those parts of the country, so we're working with the utility on reviewing if that limit is consistent or not with the practices we know you can implement already. So the issue of when and how fast you need to implement solutions is becoming an issue for us because we can do it faster, so what solutions do we need to put into table faster so we're learning from doing.

MR. HEWSON: I think all I would add is that as we implemented our coal phase out we did turn to gas. We have very good gas assets in the province and had always had a history of gas plants as one of the key sources. So we've put resources in place. What the government has committed us to look to do is to work with the distributors, the transmitters, the generators and mostly with the demand management community to work to make sure that we don't need to build any more plants.

So we're now in the province much more focused on a DR auction that is going very well. Our smarter pricing we've rolled in smart meters across the entire

province, implemented time-of-use pricing and we're now looking at models that would make even more dynamic pricing models put in place. So we've really got to the point where we're saying we're not going to -- we don't forecast needing to build new gas plants. What we're looking at is making sure that we keep up with the renewables.

CHAIRMAN LA FLEUR: Thank you.

It's really quite striking listening to all of you because you're going through a lot of the same challenges that we are and the same phenomena of transformation, although at a different pace and with national goals, whereas we're coping with the additional dimension of having different climate goals in a lot of the different states, which is an interesting feature right now.

I wanted to also ask Dr. Dieter-Borchardt a question about just your -- one of the last things you mentioned was the coordination between the distribution system operator and the transmission system operator and that's something we've been talking about as we see potentially more distributed resources, starting in California, but in other parts of the country as well getting into the wholesale -- aggregating and getting into the wholesale market and how do you coordinate what they're paid in the distribution market versus what they're paid in the wholesale market and also how do you coordinate

operationally between the control centers?

And I'm interested in any lessons that you've learned. I know Germany, for example, has had an extremely rapid growth of distribution-connected resources and anything we should take from that as we figure out how our distribution centers and transmission centers should talk to each other.

DR. DIETER-BORCHARD: Well, unfortunately, you refer to Germany. Yes, it's true there we have almost 900 distribution system operators, very small ones even and serving less than 100,000 customers. So I don't think that that's the model that you should follow, but until now I must say the distribution side was left out of our development of the energy system; but as I have said already, now bringing massive renewables into the distribution grid now we have to deal with that. We have to deal with that to also reformulate the roles of the distribution system operators. We have to give them access to the flexibility because they have the first go on all the energy that is coming into their grid. And then because again we do not -- as in Ontario, we do not also want to now go for a copper plate. We also want now then to have the cooperation between DSOs and TSOs so to bring then this energy up to the transmission grid.

And what we are proposing now, so I cannot give

you the results, but what we are proposing now is, first of all, at the European level we have already a very strong European organizations, not lobby organizations, institutions representing the TSOs in gas and electricity and we have no such structure for the DSOs and that's what we are proposing now. We are proposing to establish not exactly in the same way, but similar to the GSOs, a DSO body at EU level. That's the first step.

And the second step then is, as I said, we are also tasking the platform that both organizations then have to build. We are tasking them with the different tasks where we then not dictate how they should implement then the cooperation, but we say on which fields they have to cooperate. For instance, data management they have to do, then the integration of the renewables, the planning and managing.

Cybersecurity these kinds of issues they have to work out codes and guidelines where necessary, demand side management the same thing. So all this they have to work out then in future from this platform and then it goes through the normal process. So it is a structural approach and task approach, but selected tasks.

CHAIRMAN LA FLEUR: Thank you.

I wanted to turn to our colleagues in North America here. Of course, Mr. Hewson, Canada's been a part

of NERC since its creation and we run an integrated grid. And Commissioner Madrigal, I know you recently signed a Memorandum of Understanding with NERC and have become more and more integrated with the NERC work. And by the way, I'm just struck by the fact that you're doing in Mexico things that it took 20 years here from opening the grid to setting up the market to introducing competition in transmission and everything in such a short time. It's just quite impressive.

I'd like to turn back to the conversation we had in the session before and ask Mr. Hewson and Commission Madrigal what you're looking for from NERC as you go through this transformation? We're all going through an energy transformation, but how this NERC and energy reliability enterprise can help and anything you want to contribute on that topic because we see you as partners in this topic we're working on today.

COMMISSIONER MADRIGAL: Yes, thank you.

I think for us cooperation is very important. We learn a lot. Our energy systems are more and more integrated. Of course, they are more integrated in the gas and liquid fuel sector, but what integrated in gas -- basically, what integrated in electricity is 40 percent of our production is from gas, so without recognizing that even at the ministerial letter Mexico signed with the DOE this

general principle for promotion the reliability, then we with the system operator and NERC sign them and will -- understanding we were already receiving lots of very valuable feedback from NERC. You know practices on reliability, sitting a standard, how to supervise, and basically the objective of this memorandum is to exchange experiences on physical infrastructure protections, cybersecurity operation and planning. So it was just basically for us a new step in the relationship because it has been so useful.

One of the areas that I see of importance going forward is with the opening of the power market in Mexico we see a lot of more interesting trading across borders. We have a historical interconnection with California and their collaboration has proven there it's always beneficial to both parties if we have common rules, common reliability standards. There in California we use many of the WEC standards. So going forward, I just see our two markets deepening a lot. We have many hearings at the Commission with in depth opinion from the U.S., from the different states trying to build transmission infrastructure to trade energy to Mexico.

So we need to, I would say, work a little bit more closely on cross-border capacity location, transmission rights, and of course, reliability standards as integration

gradually grows in other states. So I think it's just a natural progression similar to what you have seen in Mexico. But I just wanted to stress that the relationship has been very, very useful so far here.

CHAIRMAN LA FLEUR: Thank you. Mr. Hewson?

MR. HEWSON: Thank you. So I would second Commissioner Madrigal's point about inter-ties. I know that as we look the planning that the IESO is doing for Ontario the inter-ties play an incredibly important role both ways. You know we're an importer and exporter every year. And as we look at developing the renewable -- greater renewable energy in the system that becomes even more important for both sides, for New York, Michigan as they're developing their climate goals and they're implementing their new polices we want to be able to make sure that we work well together.

So I hope and understand from my colleagues at the IESO that NERC is taking those things into consideration and is considering the need for good flexibility across the systems to be able to integrate the changes in the way the supply situation is working. I think going forward the DSO side of things is going to become more critical for -- I know our ISO is much more closely working with them. I think that will slowly work its way up and there's going to be more coordination across those systems.

And I guess I would say, as an economic regulator, we're always looking for the standard-setting body to be taking into consideration that care about the costs of compliance, the cost of implementing new standards, recognizing that as the supply changes there are new cost pressures in the system, either from the renewables themselves or the different systems that have to go into place like storage to be able to make sure that you can manage that. And so we're constantly, as the regulator, looking to make sure the system is as efficient as possible.

CHAIRMAN LA FLEUR: Thank you. I want to turn it back to Michael, who actually has some recent experience in the European Union on an assignment, so I'm sure you'll get some staff questions.

MR. BARDEE: On my assignment, I was actually reporting to Klaus Dieter, so now it's payback time. And I actually do have a question for you, sir.

As you may know, in our country one of the issues we are facing now here at FERC is how to balance preferences of states to manage their resource portfolios to make their preferences known on generation and other resources, how to balance that with having regional markets and not having those markets distorted by the inputs by individual states.

You described briefly your proposal on capacity

mechanisms, which are, in sense, are tools used by member states have to integrate in some way with the regional cross-border markets that you're hoping to encourage. Can you talk about how that proposal is fairing so far?

DR. DIETER-BORCHARDT: Yes, thank you very much.

This does not necessarily mean if you have the energy mix left to the member states and you create a regional market that this is distorted. It becomes distorted when the member states put money into the development of one or the other technology and that is the point because you can have different energy mix in a region. Here a region means different members states together in a region and each member state has a different energy mix. This can perfectly work and we have the rule to make it work, but the biggest enemy is the state intervention in the national context, which then, of course, has a direct impact on the regional market and that's we have revisited the support schemes for renewable. I tell here example Germany. By the way, Ms. LaFleur, that's maybe a lesson learned not to repeat, what the Germans did. They were successful to boost renewables, but at the price that no other country can afford, so -- tariffs 20 years at a very high level is not the way to go.

We have changed the system. There is no feed in tariff any more allowed, so renewable support scheme have to

be market-based. They have to be auctioned and the price has to be tested through the market. So this is on the support scheme.

You mentioned the capacity mechanisms. It is a subsidy scheme, not doubt about it. That's the reason why we have said first the necessity has to be established at the regional level, not at the national level. Let's assume that you have in the Country A you have an adequacy problem, but next to it in the Country B you have a mothballed gas-fired power plant. It is not invented Belgium/Holland. Belgium has an adequacy problem because they have problems with their nuclear plants.

Next, 16 kilometers from the Belgium grid, there is a mothballed Dutch gas-fired power plant, so use it, make the connection, and use it. Here we had struggled with the Belgium government because they said, no, we don't trust the Dutch, so we want to have our strategic reserve. So all this comes in, but here, of course, that's the role of the Commission then to go into that and saying, look, this is the kind of state intervention that we cannot accept because let the market work. Because if you have the connections and you use all the potential of the regional market, then you get very, very good results, cost-efficient results, so adequacy assessment for the capacity mechanism regional level.

The other issue is there cross-border participation. So if they are allowed to design a capacity mechanism, it cannot stay national so others can offer because they have to tender. These are the elements that we are, from the European level, bringing into avoid the risks that you rightly pointed to, that if you have this -- every country has its champion and is going for it and supporting it that would have a devastating effect on regional market. So therefore we have a very strong state supervision by my colleagues from DG competition. You all have certainly heard about of them, so that's one of the tools.

And the other we are doing through the energy policy that we are trying to Europeanize support schemes whenever they are necessary and we are going for regional assessments instead of national assessments.

MR. BARDEE: One other question on a different topic then for any of the panelists. One of the issues that we have done some work on and may have more to do is as renewables continue to grow on our system we've tried to ensure that they are contributing the services that other generators provide, whether it's a primary frequency response or voltage or other services so that at an appropriate time and in appropriate way they are asked to bear their share of the burden just like other generators, and I wonder how you all are doing with that issue.

MR. HEWSON: Certainly, at the transmission level the IESO has been working with the large transmission connected wind facilities to look at increasing their ability to provide some of those services. At the distribution level, I think that's the next area that we're going to get into. Right now they've connected. The distributors have really taken on the role of upgrading their systems to be able to make sure that they can manage the effect of the renewable energy on the system. So I think it's an area that we're going to get into more, certainly being talked a lot about in Ontario, the need to make sure that all generators are providing the same types of services.

COMMISSOINER MADRIGAL: On the technical side, what we did as part of the first sort of independently set grid code, we review what has been Germany and Spain and the U.S. and there are very specific technical requirements on low voltage, ride-through capability, frequency response. So from the beginning we already included some of those more than requirements for large scale facilities because the experience of the past 10 years was that, yes, we need to improve. You know we had some all-induction machines, so we're moving to new technologies.

On the technical requirements also of the distributive level, we have a back-and-forth with the

utility with regard to inverters, so the issue of smart inverters. So we had a long discussion what is a smart inverter. Are you going to be able to use it where we ask the solution utilities, so the utilization part of smart inverters and the abilities you have to send signal I think it cannot be overlooked because we say we put all these requirements are you going to be able to use them or not. So we reached to a compromise in which we set some smart inverter light requirements for distributed generation resources in terms of the frequencies they have to stay connected or disconnected from the system, but I think the distribution level is going to be a learning process because not all distribution utilities are at the same level of maturity to use those technologies. Some utilities we saw in Mexico were struggling on how to understand then metering, the rule. How do I calculate the bill? How do I send the calculation, basic stuff? So when you move to the -- of the controls, it becomes a little bit more complex. So I really think, as our colleague from Germany, we need to work more on making sure distribution utilities work together to understand this new world in a more organized way because I think that's definitely a challenge.

On the commercial side, and although we're really moving really fast with the reform, on the pricing on ancillary services, they celebrated the work we were doing

on pricing, especially frequency response and reactive power because we have seen a tremendous interest of consumers to install storage, even medium scale. And you know for storage to say I want you to recognize the value I'm providing to the system. So we're thinking more realistically on how we should price ancillary services, so that any device if it is a storage or if it is a wind or solar plant is priced accordingly, so we haven't finished that yet. So we are working and I just thinking on how to do it so that the value provide by storage or wind or solar is recognized regardless of what technology is providing the service. So there we still have a pending task and we're trying to just learn as much as we can.

DR. DIETER-BROCHARDT: We as well. We are going first and foremost to the DSOs for the reasons that I have mentioned. Most renewables go into the distribution grid. That's why they need to have the access that they currently do not have to the extent necessary. But next to it, we want also to develop a market for our ancillary services so that we do not see that DSOs should have an exclusive right in providing these services.

Certain, yes, those are anyway covered by our network codes, but other services can also be provided through the market and therefore we are also very keen to develop certain ancillary services over the market and then

the rest producers, of course, they have to pay for it because they remain responsible if they cannot. And they cannot carry out this task themselves. They have to purchase the services over the market or if they get it from the DSOs, then of course it is included in the fees.

MR. BARDEE: Okay, so let me thank our three panelists and we really do appreciate your being here today, coming farther than anyone else on our agenda today. We thank you. And we'll come back at hour from now, 1:35.

(LUNCH BREAK)

MR. BARDEE: Thank you everyone. We are back for Panel Number Three headed as the Potential for Long-Term and Large-Scaled Disruptions to the Bulk-Power System. So I will start us off with our panelists, starting with Mark Lauby from NERC. Mark, please take it.

STATEMENT OF MARK LAUBY

MR. LAUBY: Thank you and good afternoon. I wish to thank the FERC Chair and of course Commissioner Honorable and the staff for holding the Reliability Conference.

At no point in modern history has the electricity sector experience a period of such revolutionary change. As to the theme of this panel, avoiding long-term and large-scale Bulk Power System disruptions is at the

heart of what NERC's mission is. In fact, NERC and the regional entities work with industry every day to identify risks to reliability, prioritize actions, and implement mitigations.

NERC uses a number of mechanisms for risk identification and mitigation. For example, the Reliability Issues Steering Committee identifies, prioritizes, and recommends mitigation of high and medium priority emerging risks. Some of the indentified risks include the changing resource mix, loss of situation awareness, extreme natural events, and cyber and physical security vulnerabilities. I'd like to focus on two issues related to the changing resource mix, distributive resources and single points of disruptions.

As Gerry mentioned earlier, the ERO Enterprise continues to scan the system for information that its collects for looking for faint signals, finding and addressing small risks today so that they don't become a bigger one tomorrow and this is, of course, evidenced by our recent technical report in the alert and affordable -- generation.

NERC will continue to scan for affects on the Bulk Power System, including monitoring the proliferation of distributive energy resources. We will focus especially on the changes in system characteristics and ensuring that

there are sufficient amounts of essential reliability services.

Secondly, suspending the supply of natural gas in the Aliso Canyon storage facility is a good study case on the vulnerabilities at the intersection between electric and natural gas industries. As an in depth review of this risk, NERC is completing a study on single points of disruptions, recommending, first, FERC run gas transportation as a reliable supply mechanism; secondly, periodic verification of dual fuel capability and availability. I understand it's getting harder and harder to build dual fuel plants; ability to obtain air permits or waivers to them anyway and increase planning activities, contingency analysis, and operational coordination between the two sectors.

I'm going to transition a little bit to resiliency. System resiliency is becoming an enhanced yardstick for reliability and I will cover resiliency in the context of two additional risks, one being extreme natural events and the second the loss of situational awareness. FERC, NERC, and regional entities are actively working together jointly on resiliency. In 2016, FERC and the ERO Enterprise jointly issued a report reviewing the sampling of industry restoration recovery plans. The report concluded that the plans were thorough and highly detailed and included 15 recommendations.

As a follow on to that study, a recent study was completed looking at the loss key situation awareness capabilities and how they may impact system restoration. Restoration activities that maybe difficult without these capabilities were identified, along with provided recommended methods, practices, and training.

Another example is the mitigation from the affects of space weather. In response to the Commission's directives, NERC developed two standards to address risks from geomagnetic disturbances. The first standard requires entities to have operating procedures that mitigate potential grid risks from geomagnetic disturbances. The second standard requires system planners to address risks from geomagnetic disturbances in system design and operation.

Further, NERC recently submitted to FERC a preliminary research work plan requiring an extensive multi-year effort using scientific and technical expertise from a variety of disciplines.

So in conclusion, and I know that's what you've been waiting, NERC's leadership role is essential to maintaining a focus on conventional risks, while anticipating emerging risks during a period of revolutionary change to the electricity sector. By putting a spotlight on key risks and their mitigation, working with industry and

with all our stakeholders, the ERO Enterprise endeavors to ensure a highly reliable and secure Bulk Power System.

So thank you for the opportunity to address these important topics and I look forward to discussions.

MR. BARDEE: Thank you, Mark. Next, we have Dede Subakti from the California ISO.

STATEMENT OF MR. DEDE SUBAKTI

MR. SUBAKTI: Thank you. First of all, my name is Dede Subakti. I'm with the California ISO. Thank you. Very honored to be invited to the nerd and geek party and I'm very proud to be a geek myself. And of course, it's really hot here today, but it is much nicer than being in California, where it's actually 110 degrees.

So today, I really only have two remarks really and the first one being the gas/electric coordination and we've been talking about Aliso Canyon since, what, it feels like forever now and the need to recognize how gas and electric coordinations and the need how to recognize gas constraint in the electric system itself. And the second portion is about the emerging issue relating to the inverter-based resources, the one that we've just been talking about with regard to the Blue Cut fire.

Really, each of these topics underscore the importance of a balanced portfolio, a balance resource mix that can provide essentially reliable services to support

operation of the Bulk Power System. So let me go to the first topic with the limited operations with Aliso Canyon. It's a concern for both gas customer as well as electric customers simply because that gas curtailment through generators could or may result in electric customer interruption.

So in the past few months, I myself, learned how important it is to have a robust coordinations between regulatory authorities within the state agencies as well as with the operating entities, so I made good friends with my peer at the SoCal Gas and working closely together as we're developing a lot of operating procedures with regard to outage coordination, for example, between the gas outage and transmission outage and generation outage. Day-ahead planning, that's another one and real time operations.

We actually learned quite a bit about how each other do our business. That's very interesting and very crucial. Really, life is never the same again in California with the limit operations in Aliso Canyon.

Now last year the Commission actually authorized California ISO to implement various mitigation to address this very issue. One of the mitigation measure that worked quite a bit is the utilization of new constraint in the California ISO market. What it is, is that a constraint that is put into the market optimization to reflect gas

limitation in the way that we dispatch our generations. It works really well. We used it in the past winter when it was really cold and it works in coordination with SoCal Gas System.

The authority to use this constraint is actually expiring at the end of November 2017, so currently California ISO going through stakeholder process to explore the extension of this authority in a more permanent basis and we also exploring the need and benefit to expand the use of this constraint beyond just Southern California, such as maybe in the western energy and balance market, the EI market.

So really based these lessons, we really request or encourage Commission staff to support and continue the efforts to look at the transmission service provider, transmission operator, market operator to implement adequate tools to mitigate gas system constraint in order to be able to operate the electric system reliably. We also believe that we should continue to foster coordination between electric and natural gas transmission operations. It's very important. We learned that we rely on each other quite a bit.

So while we have made significant improvement in gas and electric coordination, Aliso Canyon underscored a need for a balanced portfolio of resources and

infrastructures to help ensure BAs, such as California ISO, so we do not overly rely on one fuel source to meet our system need and can adjust to changing operating conditions.

While that's good, we have solar-inverter, solar. We have over 10,000 megawatt of transmission credits of capacity. In the past few months, we learned that we have a 1200 megawatt and that's just one event of many. So we have joint taskforce and in the report look for two risks in there. And based on these lessons learned, we believe it's important to have a standard, a reliability standard or clarifications of the reliability standards for the ability to ride-through voltage and frequency disturbance.

So at this time, I would like to conclude my remarks and thank everybody for allowing me to share these remarks and I'll be open and happy to answer any questions.

MR. BARDEE: Thank you DeDe. Next, we have Dr. Michael Kelly Rivera from Los Alamos National Lab.

STATEMENT OF DR. MICHAEL KELLY RIVERA

DR. RIVERA: Thank you. So David Ortiz and John Ostrich of DOEE and Eric Rolickson (ph) at DHSOCHI jointly initiated a research project at Los Alamos National Laboratory. The project's intent is to understand and model the impacts of an electromagnetic pulse generated by the detonation of stockpile nuclear devices on the transmission

and generation aspects of the U.S. Bulk Power System. The ultimate goal of this research to build the knowledge and understanding of nuclear MPs and their interaction with the BES that is necessary to develop a scientific workflow similar to TPL007-1, whereby the resilience of the USPES, the nuclear EMP can be evaluated.

At the outset, constraints were established for this scientific workflow. We would only consider a nuclear MP insult an event of concern if it causes two affects. The first is long-term damage to the BES requiring in excess of three days to repair and the second is that an impact of a significant portion of the BES resulting in an excess of $4 billion a day in loss economic activity to the United States.

We've completed the first two phases of this work and these phases, nuclear EMP insults were parameterized. You can see the parameterization on the second slide of the set of slides you have in front of you and a list of benchmark events also on Slide 2 covering this parameterization we've generated. And we've begun to determine which of the benchmark insults were most likely to rise to the threshold of the study constraints.

I'm going to jump straight to discussing the five benchmarks XO atmospheric nuclear EMP insults that are enumerated in the handout. I want to stress these benchmark

events do not correspond to any particular nuclear weapon or weapon delivery capacity. If the did, I would be leaving in an orange jumpsuit. Rather they have been chosen to clearly delineate regions of interest where certain EMP effects, for example, the E3 heave or the E3 blast or the E1 phase of the first are dominate.

I'm not going to go into the extreme detail on each of these benchmark events. Their expected impact to the BES is shown in the table on page 2 based on our current and previous studies. I want to note that there is a slight error in the table. The impact from the 25 kiloton 100 kilometer case should read a medium with a 200 kilometer case reading high. We'll get to that if you ask questions later.

I'm going to stress two important points about E1 that we are finding in our analysis and back those points up with data that is presented later on in the later pages of the handout. The first point that I'm going to stress is not a new observation, but it certainly is an observation that is not advertised well enough. Those of us familiar with EMP know about smile diagrams very well. A smile diagram is a general form for the radiated hazard field present in the E1 part of the electric magnetic pulse created high altitude EMP insult.

The E1 smile diagram for our five benchmark

cases is shown on the third page of the handout. Naively, one might assume that where the electromagnetic pulse is strongest the largest currents will be generated on cables and lines. This line of thinking leads to worst-case values of coupling, the worst-case current peaks, as shown on the next figure or the next page.

If we look at the table to the upper right reporting magnitude, for a few of these benchmark events the pulses can exceed a megavolt in size if we think about the coupling this way. This coupling, however, is completely wrong. The efficacy with which the E1 component of EMP can couple cables and lines is determined by more than just magnitude. It's determined by the phase angle of the electric field as well as a bunch of other things.

When these constraints are incorporated, the realistic coupling hazard is shown on Figure 5. I'm not going to go into extreme detail, but the important point to take from this is that the magnitudes of the fields are now down by a factor of 3 in some cases and even more. So the important point to draw from this is the necessity to have a complete workflow that incorporates all of the elements from one phase to another. You cannot just simply hand off the magnitude and expect the engineers to do coupling without any sort of context and without any sort of other constraints.

And the second point I want to make is about the konus covering EMP event. For our benchmark events, this corresponds to the 400 kilometer burst altitudes. The peak radiated hazard fields and conducted hazard fields drop off precipitously at these altitudes. For the 25 kiloton case, in fact, the radiated hazardous fields dropped by almost a factor of 5.

We are not ready at this point to conclude that this means that the konus covering events are of absolutely no concern, but we can say that the lower altitude burst events, though affecting a smaller area, have a significantly higher chance of damaging BES equipment within the area that they affect. Thank you.

MR. BARDEE: Thank you, Dr. Rivera. Next, Dr. George Baker.

STATEMENT OF DR. GEORGE BAKER

DR. BAKER: I want to thank Chairman LaFleur and the other FERC Commissioners for the opportunity to speak today. I'm a senior advisor to the Congressional EMP Commission. I'm filling in today for Mr. Earl Gjelde who is the former COO of Bountiful Electric Power Administration and Undersecretary of the Interior and he regrets his inability to attend.

I want to discuss EMP together with cyber and physical threats, the EMP Commission, the charter we're

looking at all three affects, the combined affects and what I want to do in the time I have is discuss a vision for the future where the power systems will be able to operate through, will recover quickly from these what we call triple three contingencies. And there's a huge possibility of common ground here. If you look at what the industry is striving achieve and what the EMP Commission there's a huge overlap and just stress that.

So the first point of the vision is that the industry and government would be working together to achieve the resiliency to these combined affects and private public partnerships are essential and there's already some very good examples of these in force. The infragard, the EMP special interest group and several public/private national exercise -- Army War College, National Defense, University NARUC and U.S. National Guard Association is examples.

Also, another good example of late is Duke Energy is working with state and local infrastructure service providers and emergency responders at Lake Wiley to develop a plan for EMP protection.

Now the U.S. Military has proven EMP protection approaches that can be translated directly to a large part of the grid infrastructure. And I'm concerned and disappointed because there's been inadequate sharing of the DoD insights with the power industry and DOE and EPRI and as

a result there's a lot of work that's being done that's really reinventing things that were already known and that's a problem. That's going to complicate the playing field.

The second point in the vision is the electric utilities is able to recapture the cost for protection. And here I'm not going to go into any detail because Tom Popik will cover this.

Third, we need better models, national-level models of grid affects and recovery steps and I think Los Alamos is already onto this, but in order to have priority system hardening, safe shutdown, and expedient reconstitution we need better models and model development will be greatly aided if industry historical databases are made available to us. We have also yet to perform test to failure validation for large transformers and generator stations. That'll be every important to know where these things actually failed.

Fourth, a vision point is a coordinated national level Black Start Plan and resources that are exercised on a regular basis. We have Black Start plans mandated for limited blackout contingencies, but there's presently no national plan addressing restoring the grid following a large, long-term outage. A big difference between a normal Black Start, if you want to call it, and a long-term outage Black Start is the absence of functioning neighboring

regions. So when you get into local preparedness, it becomes all the more important there.

Also, the communication assets used under normal conditions will likely not be available due to EMP and GMD affects, such as land mobile radios and UHF SATCOM maybe the only communications available and these constraints need to be included in planning and exercises.

And finally, we need -- and this is a point that Commissioner Gelde (ph) wanted me to stress that the FERC/NERC Consortium is not set up administratively or legally for national security problem resolution. And we believe on the Commission that a national electric power protection executive is needed, reporting to the National Security Council and that executive should be vetted with the authority to establish protection and assessments guidelines.

So those are the points. That's the vision. And I hope that this will help focus our efforts to protect the grid. Thank you.

MR. BARDEE: Thank you, Dr. Baker. Next, we have Dr. Randy Horton from EPRI.

STATEMENT OF DR. RANDY HORTON

DR. HORTON: Thank you, Chairman LaFleur, Commissioner Honorable, FERC staff, and fellow panelists, EPRI appreciates the opportunity to participate in today's

technical conference. So my comments here today are going to address the question that was posed to the panel regarding manmade electromagnetic pulse. I will provide a brief overview of the work that we're doing as well as some of the knowledge gaps we're attempting to address with our research.

So April 2016, EPRI initiated a three-year research project to address the potential threat of how altitude to the resiliency and reliability of the Bulk Power System. And today I'm pleased to say that the project has financial support from nearly 60 U.S. electric utilities.

I will refer you to my written comments regarding the details of our research plan, but the primary objectives of the plan are, one, improve understanding of the potential impacts of altitude to EMP and we're looking specifically at E1, E2, and E3 on the Bulk Power System through extensive laboratory testing and computer-based modeling; secondly, develop software tools, techniques, and guidance that could be used by utilities and others to help assess the potential impacts of HEMP on individual assets and the Bulk Power System as a whole; three, to develop cost-effective options to help mitigate the potential impacts, and fourth, to provide timely communication of our research findings to our supporting members and stakeholders, as appropriate.

Through our collaborative research model, EPRI is bringing together experts in electric power systems as well as those versed in the phenomenology and effects of -- EMP to improve threat assessments to the Bulk Power System. For example, we're working closely with the Department of Energy, Lawrence Moore National Lab, Sandia National Lab, and Los Alamos National Lab, which I can say Mike and I've become close friends over the last year or so. And we're also in communication with other agencies, such as FERC, DHS, and the Defense Threat Reduction Agency or DTRA.

I will now quickly transition to our E3 assessment that was published in February of this year. Due to concerns expressed over the potential loss of a large number of bulk-power transformers which could lead to a long-term blackout, an initial focus of our research was to determine the potential impact of E3 on these assets. The EPRI Study evaluated the potential impacts of E3 from a single altitude nuclear detonation over 11 different national target locations in the continental U.S.

Details of the study are provided in my written comments, but in short, the results of our study indicate that although a significant number of bulk-power transformers could experience GIC levels above 75 amps per phase or more, and that's the screening criteria that's in CPL7. Only a small fraction, 3 to 14, depending on target

location evaluated would be of potential risk of thermal damage.

These results can be used to help quantify the overall risks of E3 impacts on the Bulk Power System, but I want to stress that they should not be interpreted to indicate that E3 will not affect Bulk Power System reliability. The potential for widespread outages due to voltage collapse and the combined affects of E1, E2, and E3 together are still being evaluated. Although, the E3 research is continuing, a significance focus of EPRI's research efforts in 2017 and beyond are related to assessing the threat posed by E1 and E2 and developing the capability to evaluate the combined affects of E1, E2, and E3 simultaneously. We believe that the latter capabilities is vitally important in understanding the true impacts of HEMP on the Bulk Power System.

In conclusion, the potential impacts of HEMP are real; however, there are many open research questions that need to be answered before risk-informed decisions related to hardening and mitigation can be made. EPRI is committed to developing science-based solutions to these difficult problems and will continue to offer technical leadership and support to the electricity sector, public policymakers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity.

Thank you again for the opportunity to be here today. This concludes my testimony. I look forward to any questions you have.

MR. BARDEE: Thank you, Randy. Next is Tom Popik from the Foundation for a Resilient Society.

STATEMENT OF MR. THOMAS POPIK

MR. POPIK: Thank you Michael Bardee. And at this point, the usual thing is for the panelists to thank the Commission for the opportunity to testify. In this case I would like to doubly say that. The Foundation for a Resilient Society is usually a dissenting voice, but for the second year in a row we've been invited to testify here. And I would just say that open debate is alive and well at FERC.

I can sit next to Dr. Horton here and we can have a debate in public and that really reflects very well, both on FERC and our country. And so I'll just briefly say something about Dr. Horton's testimony. In terms of the 3 to 14 transformers that would be impacted, we really have a small base of real world tests for that conclusion. Is it correct there's only two actual hardware tests for transformers that that was based on?

DR. HORTON: I believe that's correct.

MR. POPKIN: Okay. So we're a great nation. We have hundreds of millions of people to protect and we really

should be able to devote the societal resources to having tested more than two transformers and not even to failure and not at full load; is that correct?

DR. HORTON: Not to failure.

MR. POPKIN: Okay. To come to these kinds of conclusions that are so important to our society. So I'll get into some of the substance to my testimony. The staff, one of the prompts for this testimony is the question of long-term outage and it's really a very important question. We have about 10 pages of testimony. I can't go through it in the next two and a half minutes, but I would refer people to the testimony, which I believe has been put online by the Commission at this point and I also have paper copies with me.

But briefly, if we were to a long-term outage, everybody in this room could potentially be in danger. What is a long-term outage? It's an outage that persists longer than the resources of backup power for the Bulk Power System and supporting infrastructures and over an area so large that significant outside assistance would be impractical. We have a scenario for actually the eastern part of the United States in my testimony today and I would really encourage people to go through that.

I have some more remarks also about what really drives reliability here in the United States and the

constraints that we, as a society, are put under. And I would start off by saying that so much of Mr. Lauby's testimony today and Gerry Cauley's testimony earlier, the Foundation for a Resilient Society really agrees with. When they start talking about gas/electric interdependence, the need for fuel diversity, and the need for spending generation for frequency support and for reactive power, especially in places like California, a lot of these technical reports that are coming out of NERC are really excellent and we do hope that the Commission pays close attention to those reports.

And also in my testimony today, we have a lot of quantitative analysis which supports those findings of NERC. And I would also say, very briefly, one of the fundamental problems is that the market, especially the organized markets, do not appropriately value reliability. And we have, again, good quantitative analysis for this in my testimony today.

And finally, on the last page of the testimony of Resilient Society, we have some very specific recommendations for the Commission and the Commissioners and we hope that they examine those closely. And I'd be happy to take any questions about those recommendations. Thank you very much.

MR. BARDEE: Thank you, Mr. Popik. And finally,

we have Sylvain Clermont on behalf of the Canadian Electricity Association.

STATEMENT OF SYLVAIN CLERMONT

MR. CLERMONT: Thank you, Mike. Bonjour Madame President (speaking French).

Commissioner Honorable and Mr. Bardee and FERC staff thank you for the opportunity to participate in this discussion about reliability and to take the time so we can have a discussion on the reliability. And it is also an honor for me to represent my fellow Canadian colleagues.

It's been said, but it's probably useless to remind anyone about the integrated nature of the electric grid, but let me do it anyway because we must be looking at solutions together. We are in this together. Today's threats, including the one we'll be discussing in this conference are cyber/physical security, extreme weather events, CMP, GMD, you will all agree are all very different. They're varied in nature. They're complex and most of them are evolving. So preparing for one does not necessarily prepare the grid for the other one. But still, we must prepare for all of these and the threats don't know yet, so solutions probably must be on the same nature. They must be varied. They must adapt and we suggest we must take an all deserved approach to resiliency instead of focusing on each of these threats individually.

So what do we do? Well, certainly, careful analysis to learn and understand the threats and their impact and the network behavior resulting from these threats is important. Risk identification like NERC is doing that is proactive action, looking forward trying to anticipate where your bigger risk will come and trying to understand what will affect your network in the year to come.

And at entities, each of us we should continue to study our studies to better understand the impact on our own network. That should result I call them intelligent investing at strategic and critical points of our network. So out of these analyses we understand where are the weak points, if I may say, of our network, so intelligent investing to make those weak points or strategic points more resilient.

Managing carefully inventory spare parts. We've been talking about spare part transformer for a while, but a bunch of spare parts for your critical equipment, so I call that managing carefully inventory and of course collaborate together, including collaborating with regulator and have open discussion with regulator. Sharing information between industry, government, and regulator, we keep saying that, but that is really key to making good progress, using the forums even more. The forums like the NATF and the GATF offers great spaces for candid discussions.

Continue and expand the exercise like the grid-x. Grid-x are a great learning experience for all of us -- government, industry -- so we should continue those and expand those.

In Canada and with the U.S., we did recently the U.S./Canada electric grid security and resiliency strategy. That's a start. We should continue to work on that and work on the actions that are in that document. We also must keep in mind that as regulator and our customers want us to spend wisely the money they give us we must be careful about where we spend to make sure that we spend on what matters most for reliability.

All of these threats, of course, including the I- impact can't be ignored, but I believe they must be addressed with broad solutions that make the grid more robust and more resilient to anything.

And finally, standards -- and maybe we will be discussing that more -- standards are not the only tool in our toolbox and may not be actually the most efficient tool in our toolbox. We have alerts, guidelines, best practices, lessons learned. Are there ways to improve on those? Are there ways to follow ups on best practices? So like alerts when they are issued, you must respond and say, okay, I did what's in the alert. Could we expand for best practices? It's an open question, but these are tools in our toolbox

and they probably can be used more.

And lastly, remember no on entity, no one agency can work in isolation to find a solution. So that concludes my testimony. Many thanks for your attention and for the opportunity and will be pleased to discuss any question you may have.

MR. BARDEE: Thank you Sylvain. We'll start our questioning with Acting Chairman LaFleur.

CHAIRMAN LA FLEUR: Thank you. Well, thank you all very much and merci beaucoup, Mr. Clermont.

Okay, I'm going to start with Dr. Horton. As you probably know, I was recently hauled up to the Hill to testify about EMP and it actually was a great experience because as always when you testify it meant I spent several days really preparing. And I testified that the Commission has been quite deliberate in not directing an EMP standard thus far as we have directed physical security, GMD, and other things because we didn't believe that we had a clear enough path to where the best place would be to require thousands of transmission owners to spend their money to protect the grid against the biggest risks. And I got into a little bit of a sparring with some of the other folks on the panel about whether the physical securities studies or whatever how we would best get at that.

And I pointed quite repeatedly to the Los

Alamos, Idaho, and EPRI work as potentially yielding that information about how we best actually protect the grid. And I see in your testimony, Dr. Horton, and I invite others to chime in too, that some of these pieces of work from EPRI are coming quite soon, third quarter this year, fourth quarter this year. Do you think those pieces of work will give us actionable information that we can use decide what to do about the grid or are they a step on a path? I mean where are we in really understanding this.

I would love to be able to do something about while I'm here, and that's not forever, so where are we?

DR. HORTON: Right. With my EPRI hat on, I have to be kind of silent on policy issues, so I'll speak strictly from a technical standpoint. So at a high level, if you're asking me from a technical standpoint does the knowledge, the tools, and guidance, and so on exists to do kind of a TPL8 type of standard I would say the answer is no.

So basically, our research project we're not really even getting into the risk piece. We're assuming that the blast happened. We're looking at really what are the true impacts and ultimately how would you develop cost-effective mitigation options to mitigate against those impacts. So we're doing this as quickly as possible, so you know this is a three-year research project, but it's not

three years of research and then the data dump. So actually, as we get to a point where we feel like we have some actionable information, we're providing that to our members. And I would also say to the public as well so as a part of public benefit mission we always evaluate our research deliverables to look and see, okay, EMP is a very important topic. Would this make sense to put these deliverables out in the public domain at zero cost? There're always in the public domain.

So for example, the report that Tom mentioned you know we did the assessment and we didn't just do the assessment and say here's the answer. We did the assessment and said here's what we did. Here's the input data we did. Here's the models we used. That's how you're able to know that two of the models were test. We're providing all that detail so that we can have these robust discussions like we're having today, but in short to answer your question, I think, ultimately, at the end of the project when we're able to do what Mike mentioned, which is this workflow, which is look at the impacts of E1, E2, and E3 together we'll have bits and pieces along the way, but we really need to get to the point where we can study all that together to really find tune what the potential hardening options might be.

DR. RIVERA: The workflow can't be understated

here. There's a lot of missing pieces to EMP, but there's also not kind of universally accepted workflow. Don't worry. There are workflows out there. IEC has a set of standards that you can follow. The quantitative workflow from end-to-end that's agreed upon is important here. I mean to go back to kind of the what happened with TPL007. TPL007 put the workflow out there and then people came in and beat up the workflow and different piece of the workflow are now being looked at and maybe we substitute a number here or we add this piece there.

The same thing needs to happen here. We need to have an accepted workflow so that way scientists can come and have a context with which to go, okay, this is wrong here. This is right here. We have to change this and allow this workflow to evolve to eventually something that could be actionable.

DR. HORTON: And quickly, one thing I wanted to add, you know it's easy enough to build a block diagram, which is the actual workflow, but the real missing piece is the actual tools, like they have to be built essentially from scratch or figure out some way to cobble together the different types of tools. That's another thing we're working on.

CHAIRMAN LA FLEUR: Well, thank you very much. I'm most concerned about E1. I certainly agree that our job

at FERC is not prevent it. Our job is oversee the construction and operation of the grid to mitigate various hazards and I think we have -- my understanding and I'm not an electrical engineer, as is probably obviously, but I believe we have our arms around E2 because it's like lightening and we've done a lot of work on E3 like things in the GMD context, but E1 is where we really need the work that gentlemen are doing, I think, to have an intelligent mitigation strategy.

DR. RIVERA: Just to jump in, E2, generally it is said that, yes, it's a lighting-like strike and we're hardened to lighting, so everything's okay, but this is an assertion and it's something that really does need to be investigated. I am not saying I disagree with the general sentiment, but it's something that has not even been remotely investigated.

CHAIRMAN LA FLEUR: Well, that makes your work even important. So bearing in mind that we're waiting quite eagerly for that work, I want to turn to the question I think Clermont keyed it up of how can we build resilience of the grid against various risks? I'm encouraged by some of the things have been done recently on transformer sharing, with grid assurance and so forth. I'm also slightly optimistic that those sharing programs will lead to more standardization or perhaps standardization. I mean I

believe strongly that if this industry knew what it wanted in terms of mitigation it could go to ABB and Siemens and so forth and they would build it because we have -- you, collectively, have a great deal of buying power. So I think we're making a little bit of progress there, although I'm happy to hear more things we could do. But I'd like to know how do we actually design redundancy and so forth into the grid.

Of course, I read Mr. Popik's testimony, but we can't turn back the clock and say we want -- we're going to live with the system that has a lot of renewables and a lot of demand resources and a reliance on natural gas. So how do we build the Bulk Electric System to be more resilient? Are there things we could be doing in terms of -- I'd hoped that the operating procedures part of GMD would help by kind of planning in advance, islanding. We have all these experts here and appreciate any ideas how we can build it in on the front end.

MR. CLERMONT: Well, if I may take a first shot. I think what we learned from our famous ice storm in the end of the nineties.

CHAIRMAN LA FLEUR: I remember very well. We weren't too far away.

MR. CLERMONT: Well, you were in New England at that time, yes, so probably a lot of your employees came to

help. And you remember that the --

CHAIRMAN LA FLEUR: As did yours come to help us many, many times in your gray trucks.

MR. CLERMONT: Thank you. But may remember that some part of the province were out of power for three months, so I think that qualifies as a long-term outage that we're talking about. Obviously, not large scale, but a fair amount where a good share of the population was living -- was out of power for three months. So what did we learn? So we took a careful look at our network and said, okay, why? And then we came with design criteria. We review and revised our design criteria, moving forward. So all new lines must sustain more ice, more wind, more of that and more of that, but that's 20 years ago. So all the new line we build in the past 20 years are stronger. They have anti-cascading towers. They're able to support more ice and we added stronger structures.

We looked at the grid and we saw that a lot of substation were already connected to another one, so we built a couple of lines to make sure that they looped so every substation is connected to more one of its friends. And we look into remedial -- what's called RAS now, Remedial Action Schemes, to see how that could help. And we're still today looking -- we performed last year another critical look at the network.

I was talking about weak points, but after 20 years of doing that where do we believe there's weak points? Where do we believe I call them intelligent investments could be made, so one more transformer there, one more line there, one more substation to make sure that there's more loops, that there's stronger structures. It's not magical, but I think it did the job.

If were to have an ice storm like the one we had or any actually extreme weather events our network would not sustain the same amount of damage. So that's not a miracle, but it's a careful, small investment, look at what was weak, and we can all do that; but we will need an open conversation with our regulators because it will require investment. And the investment when we increase load or capability of the network are usually easier to understand for everyone, but now we're talking about money to get the same service. These may be more difficult conversations with the regulators.

CHAIRMAN LA FLEUR: That's why I'm asking the question because I would like to be a champion of building more resilience and having been around this industry for several decades I find -- and I think this is just human nature. There's a tendency to respond where it happens to what happens, so Quebec is ready for ice storms, also you did a lot of work on (0:44:07.4) disturbances after that

happened.

New York City has built its substations to endure the next Sandy and bigger than Sandy. New Orleans is ready for another Katrina. They've built the best levies in the world. You go several hundred miles away and they haven't necessarily applied the same lessons. And so that's what this continental effort is about broadening those lessons.

MR. LAUBY: Just to add, to me it comes down to basic planning and risk identification and mitigation. And of course, we've been working hard on that at NERC and with industry and identifying what are some of the risks that are existing today with the faint signals that we hear and do something about them. And also looking forward as we see more and more variable generation coming online and it's going to be always synchronous of inverter-based. How are we going to get inertia out of that? How are we going to sustain frequency? How are we going to sustain voltage in that kind of world? Let's make sure we put a spotlight on those kinds of things so that we don't have to be looking in our rearview mirror saying I wish I would've known about that. So there's a lot of things that industry does to ensure that the system's reliable. They ever get a thumbs up saying -- nobody calls them at 3:00 o'clock in the morning and say, look, it worked great.

Yes, so that being said, I think we have to be vigilant. And if you read over Mr. Popik's materials, he's identifying some of these risks as they come on the system and so what do we need to be doing now to ensure that we're ahead of it so that we've been able to ensure a highly secure and reliable Bulk Power System?

DR. HORTON: I'll just make one quick comment and kind of zero in on a particular problem, but with regards to like safe transformer impacts due to GIC, either due to B3 or GMD event, I think there was a couple of things. Our recent E3 report and research basically if you look at the way we did the study transformers that were maintained properly like if you were in good condition we didn't see a lot of issues. So you know improving maintenance activities. And then secondly, a lot of utilities are beginning to include GIC specifications in their transformer designs. I think that's another kind of low-hanging fruit action time that could be employed.

CHAIRMAN LA FLEUR: Thank you. And just to pick up on something Mr. Lauby said, there's always enough money after it happens. I just want to ask one more question because I can't let you go without asking a GMD question.

COMMISSIONER HONORABLE: I was wondering.

CHAIRMAN LA FLEUR: Well, I've been closely following the -- well, first of all, thank you for the

research plan, which has quite a lot in it. And I've been closely following the budget of the U.S. Geological Service and I'm wondering -- I want to just hear how important the work that they do is to the operating protocol standard, the ongoing work plan because I had thought we were quite dependent on real-time satellite data to understand what's happening with space weather, but I have the experts here. Because it's just something I've been really watching. There's been a lot of debate about the USGS budget.

MR. LAUBY: I think that the work that they were doing, especially around mapping resistivity was extremely helpful and there are other ways, I guess, that we can get at measuring of that resistivity, but it allowed us to get a much more of a microscopic view of the resistivity and an understanding of what the ultimate -- occurrences are.

CHAIRMAN LA FLEUR: Anyone else?

DR. HORTON: I would just say that having the magnetometer data and also the Earth model data is critically important with anything to do with GMD. And even the E3 I mean the Earth model piece of that is very important.

DR. BAKER: I would echo that the Earth connectivity models are extremely important and one of the ways to get at that is to make more measurements and correlation between GIC and the magnetometer data. That

needs to happen.

MR. CLERMONT: That won't be very useful for you, but in Canada we get those data from Natural Resources Canada, so we're not depending on that.

CHAIRMAN LA FLEUR: It's useful as a good example. The kid next door does their homework on time. Okay, I'll turn it over to Collette.

MR. CLERMONT: Well then, maybe it is useful for you.

COMMISSIONER HONORABLE: Good afternoon, gentlemen. Bonjure, sir.

MR. CLEMONT: Bonjure.

COMMISSIONER HONORABLE: I'm delighted to engage with you all and I want to apologize for returning late. I was at a luncheon and the speaker was Dr. April Erickson from the NASA Goddard Space Center. Believe it or not, we were almost talking over each other talking about this very topic and how almost in vogue it is, not because it's the most popular topic, but it's because we need to be focused on it. And I want to thank each and every one of you for the ways in which you have blended you expertise.

I, too, am a lawyer by trade and so this -- I'm not an engineer, but what I do know is that scientists and engineers you work by testing and challenging and finding the proper dataset and making sure that the modeling, that

sensitivities and the futures are the proper ones so that as we get more robust data we will be able to put it into some modeling process and come out with something that we can use. So really this discussion here today has given me some comfort, Cheryl, about our course with the GMD effort. And I want to thank those of you who have participated with us along that journey.

And to our Canadian friends, thank you. When I arrived here at FERC, one of my first meetings was with you all and you reminded me about how our work impacts our friends to the north, so thank you for also engaging with us.

And to Mr. Popik, thank you because you've touched upon this open process we strive to have. That's why we have so many panelists because we know that there are a lot of views and we don't want everyone to come and agree. You all, even disagreeing at times, though in an agreeable fashion, help us carry out this work better. And you testing our thinking and the ways in which we are proceeding help us and educate us. So regardless of whether you're at the table, and I know you always do, you file those comments. Please continue to do that because it so helpful to us.

Mr. Lauby, I acknowledged to you, as you know, in the other panel with Gerry Cauley, but we're so grateful

to all of you for your work on this topic in particular because it's one that challenges me personally because we don't have years of data and occurrences, thanks goodness, that would really help better inform our work.

I want to ask a question, and it goes back to something that Cheryl touched on. And I want to first start with Dr. Horton and I want to ask any of you to chime in. And let me thank every -- in full disclosure, I served on the Advisory Committee for EPRI, but I learned a lot about the ways in which EPRI is supporting the work in the sector, looking ahead at what's coming around the corner. I was very appreciative of this particular study.

I have to tell, Dr. Horton -- I call him Randy.

DR. HORTON: You can call me Randy.

COMMISSIONER HONORABLE: Thank you, Randy.

There was quite a bit of discussion. One, I think people were excited to see it, but two, I think there was an interesting question about why start at E3? You know if you think about -- and I've had to educate myself. I have just enough knowledge to be dangerous here. If you're thinking about E1 scenarios, I agree with Cheryl. Those are the things that I tend to be concerned about, especially the early time pulse events.

E2, as Dr. Rivera said, could be maybe lighting, but he said we really need to learn more about that in order

to say for sure. And then what appears to be the most significant event, the E3, which may not happen as often, but boy, when it does it will certainly get everyone's attention. Tell me, and forgive me if you've talked about this, how did you arrive at starting with E3? And let me also say that I'm grateful that you will turn to look at E1 and E2 because I think altogether it will provide a wealth of information for us.

DR. HORTON: So we made the decision I can say, and you probably are aware of this based on what you just said about some of the discussions you've had. We had some very robust I'll say discussions about why we chose to go with E3, but really it was simple. We did realize that if you lost a large number of volt power transformers you would have a blackout that lasted for a long time and then that kind of changes the whole landscape. So right off the gate we wanted to see, okay, if we took some of the same studies that had been done in the past, but sort of update those with some of the newer modeling capability that we have, we wanted to see would we get the same answer.

Based on what we did, we didn't get the same answer and that was the reason we felt it was very important to put all of those details in a report so we can have a discussion about what we did. You know people may not agree with it, but we can talk about it and so on.

That said, in our study, we were not able to include the effects of E1 or E2, which you know if you think about how this might actually work in reality is you have the E1 come through. You may damage some electronics. It could affect relaying and how the system would respond when you'd get to the E3 piece, but we feel like our analysis was conservative from the E3 effects on transformers, but when you start to look at what the overall system impact is you really do need to include all there. So we're trying to get to a point where we can model those -- essentially, model those all together so that you really know what the full impact is. That's kind of a long answer for a short question.

COMMISSIONER HONORABLE: And I don't know if anyone else wants to chime in this topic in particular, but if not, I'm going to proceed.

Dr. Rivera, I want to thank you and your colleagues -- I mentioned to Dr. Rivera before we began this morning how grateful we are for the work of our colleagues at DOE and especially you and your colleagues in the national laboratories. We rely heavily upon your work and it's beautiful how we have come to rely upon that in our rulemakings and our decision-making and so there really is a role we all play in holding this grid and making sure it's reliable and resilient, so thank you.

I want to press on you a little bit more about the E-2 areas to the extent that you're willing to discuss this. What could we do to learn more about the sorts of events that are likely to occur in an E2 occurrence and if there are things that we should be working as regulators and policymakers in this area?

DR. RIVERA: The short answer there is I don't have a good answer for you. There's just not enough done on E2. We have E2 simulators to some degree. We have E3 simulators to get to ground fields. There is, so far as I know, no direct E2 simulator with which we could even get ground fields.

Now this is not to say that this is a difficult extension of what are currently codes that out there. It just has not been done, so I wouldn't even know where to begin on answering that, but it is some research that needs to happen to ensure that this assertion about E2 is not going to have an effect is adequately researched. So just out of an adequacy of concern, basically.

COMMISSIONER HONORABLE: Thank you. And I hope that some of your colleagues have heard that. In case they're twiddling their thumbs, they can get to work on that.

DR. RIVERA: They are well aware and they are working.

COMMISSIONER HONORABLE: Well, very good thank you. And I feel confident that if you aren't aware, then there is certainly a lack of information because you are a trusted source for us and I appreciate your candor there.

Mr. Popik, I wanted to turn to your recommendations. You teed it up and I wanted to bite. So in your pre-filed testimony, you have us lots of recommendations. Thank you for those. I'm interested in one in particular and it happened to be the last one because in it you spoke about FERC's need to advocate and engage more with Congress and the FCC regarding communications, in particular, in ensuring resilience. I take that to heart. I think a number of us, as regulators, were really aware of our lack of coordination after, for instance, Hurricane Sandy and inoperable we are in and how interdependent we are and we can't communicate about getting the lights on if the communications network isn't up and the folks in the communication sector can't do their work if they don't have energy. And so we know that there is a symbiotic relationship there.

I agree with you that we haven't done enough and especially after not only Hurricane Sandy, but any number of events that have occurred. And I wanted to ask you in particular specific recommendations you have since you've teed up the issue.

MR. POPIK: Well, thank you very much for that excellent question. Before I get into the heart of it, I would say that already FERC coordinates with another important agency, which is the Nuclear Regulatory Commission and you have that annual meeting. I think you recognize, as the Commission, the importance of that symbiotic relationship between nuclear power and electric reliability. The same is becoming ever-increasingly true for communications and the Bulk Power System.

NERC and Mr. Lauby, in his testimony, referred to this. I'll just briefly give you the history in terms of resilient communications at the FCC. With Hurricane Katrina, a lot of communications were out and it became very apparent how critical communications are. There was a post-Katrina panel that recommended great resiliency of communications and the FCC actually passed a formal rule for greater backup power durations among what are called central offices and remote terminals.

Unfortunately, there was some opposition to that and ultimately that greater resiliency for backup power was placed aside by the D.C. Circuit Court and that's really where it rests right now. I think that FERC, as a Commission, would have very significant authority if you were to go to the FCC and potentially establish the same kind of regular meeting framework that you have with the NRC

and so that's really the heart of this recommendation.

COMMISSIONER HONORABLE: Well, thank you for making it. And I recognize it's something we certainly should consider it and I'm saying this out loud because I'm sure that our future colleagues, whether or not I'm here, will take this to heart. And our engagement with the NRC is quite robust and we learn so much from one another. And even with regard to rulemaking and licensing and permitting there are just a number of ways in which we are aligned, including our work with regard to reliability and resilience.

I appreciate you harking back to Hurricane Katrina. I recall days being chairman in Arkansas at the Commission and dealing with coordinating and coordination after tornadoes and after a significant amount of infrastructure was taken down. I also when hearing you speak recalled testifying before Congress before a subcommittee about responding to severe weather events and the need for the energy sector and the telecom sector to better coordinate.

But in saying this I also would say that's why the state processes are so important too, that the first responders and emergency management and every one along the spectrum also needs to be engaged. And so I appreciate that you make the recommendation and I'll certainly keep it in

mind.

MR. POPIK: Thank you.

COMMISSIONER HONORABLE: And I believe I will yield so that the staff can ask questions. Thank you.

MR. BARDEE: Thank you, Commissioner. I have a couple of areas I want to touch on and then I'll turn to my colleagues here. One of them starts from the Aliso Canyon scenario, gas dependency as it increases in our country and more specifically, the planning that might be necessary or appropriate to foresee and prepare for similar circumstances elsewhere.

We have transmission planning standard now that, in some sense, has that element in it. It applies to transmission planners and planning coordinators and it says in certain circumstances you have to consider the loss of two generating stations caused by a loss of a large gas pipeline in a region or more than one region, so I have a couple questions about that, either for Mark, Dede or both.

One is are those the right entities to give us the kind of analysis and preparation that we need. You know transmission planners, planning coordinators, first of all, are balancing authorities who are the entities responsible for balancing resources and demand. Should they have some kind of responsibility like that?

And second of all, you know transmission

planners sometimes have a large footprint, but many of them do not. Some of them have a small footprint and having a lot of little entities, small entities do this analysis may not give you the necessary insight and results because a pipeline may affect several of them in a row and they each see only their tiny slice, which may not be the problem.

MR. SUBAKTI: So California ISO we're planning coordinators for the footprint that we have in California. You're right that I think, as a planning coordinator, we do see a lot more information with regards to how all the gas infrastructures ties into our portfolio.

One unique thing about California ISO is we are also the balancing authority, so because of the fact that we are planning coordinators and we are the balancing authority, we don't see that issue that you were talking about, but I would imagine if you are only planning coordinators and not a balancing authority you might have that issue. I would agree with you in there.

Currently, we are doing the assessment for the impact of potential gas pipeline in there because obviously again we've learned through it because we have Aliso Canyon's issue that is in there. I think we are in the right directions. We believe that there is a good -- at this point in time there's a good balance between reliability standard for the planning horizons versus what

commissioners have allowed us to do to have the market incentive to implement the constraints of the gas itself into the market optimization.

So it becomes a transparent step. Where do we need the renewable resource? Where do we need the other type of resource? Where do we need the energy storage and this other stuff, and I think the ability to have a mix of resources, mixed type fuel resources would help to reduce the over reliance on the gas. But obviously, this is one the things that has been a very good experience for us. And one of the things that we also have to look at, not just the planning of what would you if you have a pipeline that doesn't work, but then the question is what would you do if you actually have a blackout, a long-term blackout with a gas pipeline?

You know many of our black start resources are natural gas units, so we actually went through this exercise to look at which are the gas compressor that rely on electric simply to be there versus which are the compressor that are actually self-propelled that they can actually self-power through the gas itself. So that exercise is very useful for us.

MR. LAUBY: Thank you for your question, Michael. You're right there is a TPO I think, four, you know called for studying certain types of events, extreme events,

including the loss of a gas pipeline and especially if they impact more than one generator or a large number of generation. And the whole idea there is to develop plans to address those and then, of course, that moves into actually implementing some of those plans down the road becomes a closer scenario.

It's something to think about now, though, because it's becoming less and less of an extreme and more and more a shorter -- you know in our face type of event that we might want to look at that standard and see if it makes sense to have really into -- put the solutions in place, that one to five-year timeframe.

MR. BARDEE: A different topic, I have a question or two on EMP. One, Dr. Baker, I'll start with you, but others can feel free to chime in, has to do with let's suppose that some point in the future the Commission decides it's time to do a standard about EMP. It's time to require a standard about EMP. If I compare it to GMD, it's a natural event and you can put a number out there for GMD and say protect to this level and you don't have to worry about the sun reacting and saying I'm going to get bigger and hit the Earth harder, but if it's an adversary, a nation state or otherwise, if we specify a level of protection in a standard for EMP, is it a concern that adversaries may respond to that? Is that a risk?

DR. BAKER: I would say because of some of the limiting effects of the atmosphere, saturation affects we call them, that you can develop a bound that would be very difficult to exceed. For instance, we've done calculations in developing the DoD standard where we varied the yield by three orders of magnitude and noticed only a factor of 4 difference in the peak field. And so for E1, I think that's not a problem. For E3, again, it's very yield dependent, monotonically yield dependent, but we know what's in the stockpiles and so we could set our standards that bounds the E3.

The Europeans have the International Electric Technical Commission. It's already published some international standards, which, at least for E1, I think would be a very good one to adopt.

MR. BARDEE: And following up on what you just mentioned about the IAC, I've read there are standards there. There's the Mill Standard, MIL, from our Department of Defense, but I've also read that those are not generally developed with the grid in mind, may not be necessarily the best approach for the grid and also might be fairly costly if they were required. And I just wonder what your perspective is on that, whether those standards have some suitability or is there anything we can learn? Any part of them we can take and use here as sort of a no regrets.

Let's start with that.

DR. BAKER: Well, for the environment, you know DoD has all kinds of infrastructure and systems out there, so the environments are independent of that where it gets to be -- or the system affects in the grid and the grid itself comes into play is when you start talking bout coupling, but I think the environment standards you could develop some that would be universal.

DR. HORTON: So I would agree with the environment piece. I think where the difficulty comes in is you've got several things playing here. You've got the environment. You have the coupling piece, which would be the modeling aspects, but then you also have this piece, okay, you can sort of calculate what you think the equipment would be exposed to during a particular event, but would it be damaged? And then also what can you do in order to kind of mitigate that damage. I think that's where the questions for, for example, substation hardened equipment. There's questions around what would the equipment actually be exposed to and then what would the potential damage be. Once you know that, you can kind of back into what the mitigation options are.

Right now you know Mil188125-1 would assume that the equipment you're trying to protect is not very hardened at all, so it's pretty robust protection. So that gets to

be very costly, so what we're trying to do from our research perspective is, is there a way to still get the same level of mitigation because you're trying to harden different kinds of equipment and do that in a more cost-effective manner. But right now there's a lot of research to be done in order to get to that point.

DR. RIVERA: So if I could just chime in, I'm going to harp on this yet again. The answer to your question is workflow related. We don't have an accepted workflow. And when I say workflow that's not just a matter of, okay, these are the steps we do to get a quantitative answer, but that also is what are the bounds of what we are calling damage that we're concerned of?

Until we have that accepted workflow, until we have the appropriate bounds for what we're actually concerned about, we don't know which parts of the IEC standards or the Mill standards we need to pull out and plug in to the workflow to establish, okay, well this is the appropriate workflow and we can use this part of the standard, so it's workflow related again. Until you have a defined workflow, I don't I can't help answer you that question.

MR. BARDEE: So my last question before I turn to my colleagues or others, and your answer was actually a good setup for it. Let's suppose we get to the answer where

that workflow is now done, we know the answer. We know what we want to do. I assume there is a big, big difference in cost of installing it in something new you're building today compared to a retrofit of a substation or a control center or anything else that's big. And assuming that we have the flexibility to actually impose standards on new stuff without mandating the same treatment for old stuff, would that be a reasonable thing to do?

DR. BAKER: I would start there. And I've read that in the next 30 years we're going to have a 50 percent build out or increased build out in the grid, if that stat is correct.

The other point I would make is the DoD experience is that if you want to do global shielding for a new build versus a retrofit, there's a factor of 10 difference in the cost, 2 percent versus 20 percent it's roughly. But there are in some cases, for instance, in a substation control building you may be able to isolate the electronics in a very small volume, in which case the protection costs would be much lower. So there's ways to protect existing equipment, if you're clever, that would not obey that factor of 10 ruling.

DR. HORTON: Just one thing I would add, cost aside, I think when we start applying some of these hardening principles and practices in substations, I think

we've got to be a little bit careful about some of the potential unintended consequences, particularly when you start to look at applying HEMP filters to CT and PT circuits and things like that.

I'm not saying we can't engineer around those, but I think just kind of blindly applying some of the hardening could potentially cause issues that we need to vet out and make sure that's not a potential issue.

MR. ORTIZ: Thank you, Mike. Thank you all for your testimony and for the lively discussion.

I want to bring up just one question regarding an item that Tom Popik put forth in his testimony -- in his submitted comments rather. And this has to do with the notion of resilient versus non-resilient capacity, meaning simply that fuel is stored onsite. This could either be I guess a dual fuel facility with some fuel stored onsite or alternatively a coal-fire power plant or a nuclear power plant and there's a suggestion in the testimony or rather in the submitted comments that somehow we should come up with more effective ways of measuring and valuing that resilient capacity in some way.

And first of all, I'd like Tom to make sure that I didn't misrepresent his remarks and also I'd like the panel, perhaps Mark and others, to comment on that notion and potentially could be done about it, either here at the

Commission or within industry. Is it more than just smart black start planning? Is it something else beyond that? Help enlighten us on what potentially could be ways to think about that kind of resilient versus non-resilient, whether or not there's a valuable way of putting it. Help us understand that, whether or not that makes sense or that's something that could be a potential area for action.

MR. POPIK: I'll go ahead and get us started off because I would like to throw out some numbers about how severe the reduction in the resilient generation capacity has been. So just to reiterate what you said, if there's fuel stored onsite, the generation capacity is resilient to short-term interruptions in fuel supply. So this would be a hydroelectric plant, a nuclear plant, a coal-fired plant with a large coal pile or a gas-fired plant that has dual fuel capability that would have oil tanks that could run for, say, 24 hours or 48 hours, so that kind of thing.

And so what we did is we went to the EAI data and we looked at two different points in time. We looked at 1996 and we compared it to the most recent data available, which is 2015. So in 1996, 97 percent of U.S. generation capacity was what we would call resilient, that had some degree of fuel stored onsite.

And when we get to generation that's been added to the system, 1997 and later, on 27 percent is resilient,

according to that definition and in some states the reduction resiliency has been especially extreme. For example, in California only 7 percent of the newly added generation, which is almost entirely gas-fired, is resilient or dual fuel. And you can actually go around and visit plants and you can see the old oil tanks that no longer have fuel oil in them.

So what's the solution to this? It's very difficult to solve this problem with reliability standards. And this is where FERC has a tremendous advantage in terms of also being the economic regulator and being able to set certain conditions of tariffs. And so one of the things in our written tariffs testimony we suggested that perhaps there could be some adjustments to the capacity markets where there could be some allocation of capacity set aside for resilient or dual fuel type plants.

MR. LAUBY: Conceptually, I think I'm really quite comfortable with the definitions, remembering that NERC has been looking at this problem for quite some time. When we looked at the Clean Power Plan and how many plants were going to retire and what are the implications of being single threaded on gas and that's why we have a report on single points of disruption and pointing to what are the potential impacts. And in fact, in our LTRA, we're starting now to get to the point of saying, well, we want to

know how many of your plants are dual fuel? How many of your plants are buying on spot or firm so that we can start getting a real idea of the size of the problem, as Mr. Popik's pointing out and what are the implications on reserve margins. How we can get an expected value of gas for not being available? We can kind of play around with that. So from a planning perspective, the methods are there and then you can start looking at what the implications are and what the value to reliability is of each one of those resources.

MR. SUBAKTI: With regard to California ISO, we do look at our black start resource, black start capable resource carefully. And you're right there's specifically one black start resource that remain -- capability. There are quite a number of black start capabilities that are hydro-based, but there are also some that are natural gas.

Now for those that are natural gas, we have to go back and make sure when working with the gas company to look at whether or not the delivery of the gas would rely on the electricity. We want to make sure that they do not rely on electricity because they have to be on a compressor site that is self-working in there.

But beyond that, we have also worked with different technologies. So for example, we have a quick start capability from a HVCD line. Normally, HVCD lines are

not for black start, but we've worked with manufacturers, with Siemens and what not to have the ability to have a quick start for the area of San Francisco because, as you know, there is no more conventional generation in San Francisco, so we look for technology improvement.

The other one that is going to be interesting is that through the -- process in there one of the measures was try to look at the potential of coupling battery storage and be able to work and help to start some of the unit that may need to be quick start. So I think we have the right people to take a look at all the solution. Dual fuel maybe one of the solutions, but I think there are -- maybe there are other emerging technologies that could actually help us towards the solution.

CHAIRMAN LA FLEUR: I guess if there's one minute, I'll ask one more question while I have all these resilience experts. Something we've been hearing a lot about is analog backup. I know it related to cybersecurity, but it might relate to E1 and communications as well. Is that something you see as part -- you know that there's a King Risch bill and so forth and the thought of -- I have to admit when I first heard it I was originally kind of skeptical, but I've kind of warmed to the thought of some different modalities of communication or ways to run the system. Is that something NERC has looked at or thought

about?

MR. LAUBY: I know that like in the recent study that we did, the joint study with FERC on the loss of many of these are communication or situation awareness, and also we went through and identified some of the different types of communication methods. You can be using satellites and cellular. Of course, cellular could be gone to. It depends on how far you go. Pretty soon you've got a cup with a string on it, but I mean at some point you know have maybe microwave and other technologies that you can use. So it's an idea especially to practice these different types of drills and then really look at which are the most resilient communications that you want to count on.

CHAIRMAN LA FLEUR: Well, the companies used to have those -- what were they, megahertz systems and the trucks with the push to talk before the cell phones.

MR. LAUBY: Yes. So it might be worth having those on board. And I want to have people on each one of the substations. How are they going to communicate with those folks?

CHAIRMAN LA FLEUR: When you picture trying to put the grid back together, it seems handy.

MR. LAUBY: Yes.

MR. POPIK: There's one instance where retaining analog capability would be especially important and it's at

the large hydroelectric facilities. Those are almost entirely plants that were built, say, 40 or 50 years ago with original analog controls. Some of them have converted over to digital, but if the old analog controls are still left in place, and importantly, there's practice or drills using the analog controls that could make a much more resilient grid and that's, as you said earlier today, that's one of the key words, how do we ensure resiliency, and one of the ways is by keeping some of that old, resilient analog capability.

CHAIRMAN LA FLEUR: I mean that was a stupid example, but I'm sure everyone in this room has a manual can opener somewhere in their kitchen.

COMMISSIONER HONORABLE: I mean it never doesn't work. It always works. So whenever that electric one screws up, and it always does -- sorry, whoever makes them -- I go to that manual one.

MR. CLERMONT: But you're right. One of the paradox of what you're talking about is one of the driver behind going digital in our substation is the loss of expertise on analog. All our technicians that were born and worked for a long time retired -- with analog -- pieces are retiring, so that loss of expertise is something that we're concerned about and it's kind of giving an incentive to move faster towards digital. And Mr. Popik's right. I mean all

of use our network infrastructure was not built all last year, so we still have that, but we're losing fast the expertise on that, the spare parts, and everything and that's an incentive to go digital. But maybe we will revise that, revisit that in the future.

CHAIRMAN LA FLEUR: Thank you.

MR. BARDEE: With that, we'll wrap up this panel. I'd like to thank all of you for your time and for your very thoughtful comments. Thanks. And we'll be back at 3:15.

(Break)

MR. BARDEE: Our panel now is addressing the topics of cybersecurity and the CIP standards and other efforts that might be helpful in terms of better protecting the grid from the risk of cybersecurity. So I will start by turning to Marcus Sachs from NERC to lead us off.

STATEMENT OF MR. MARCUS SACHS

MR. SACHS: Thank you, Mike. Good afternoon. Madame Chair and Commissioner Honorable, thank you for having us and for the opportunity to appear before the Commission and staff and others to discuss grid security, also the work we're doing at NERC and with the electricity EISAC to mitigate potential impacts to the Bulk Electric System.

I think we all know that assessing risks and

assessing the security state is hard. It requires dynamic of constant vigilance and agility. The threats continue to evolve, particularly nation state threats as well as criminal threats and others as society changes and as the world dynamics change so do the threats, so that attention to detail, of course, is very important.

At NERC we address cyber risk through a variety of regulatory and non-regulatory means. Our mandatory CIP standards, which you all are very familiar, are our foundation for where we start with security. They provide universal baseline protections, but because that ever-evolving nature of threats standards alone cannot stand up to that challenge. We have to do other things. We have to have vigilance. We have to respond to these new and changing events.

We also have at NERC the Electricity Information Sharing and Analysis Center or EISAC, which serves as an information-sharing conduit, which when the electricity industry and the government for cyber and physical threat exchange threat analysis and understanding what's happening.

The EISAC facilitates communication of important or actual information and we strive to maintain what we call the ground truth, the actual information about this rapidly evolving security world. Together these mandatory

standards, effective information sharing, working together provide a very robust and agile toolset to help us protect the Bulk Power System.

In addition, we also work very closely with our partners at the Electricity Subsector Coordinating Council or the ESCC, very unique to our sector to have the CEOs involved in security discussions and I think we have a very, very, very strong public/private partnership that's important to addressing this security world.

Let me just briefly walk through what we see as -- and the EISAC has learned a lot about security over the last couple years as we continue to grow and change, but there's probably five major areas we're concerned about that the grid needs to worry about and this is just cyber. I think we all understand the physical challenges that are out there, but we see a lot of cyber stuff that began years ago with more of a reputation problem protecting websites -- you know phishing, stealing domain names. That's an inconvenience problem, but I think it's something that as long we're very aware of it and we're tracking, certainly it's something we can handle.

But we've also seen the criminal world move into theft, both theft of intellectual property as well as theft of value. This is the old FBI thing -- you know why do you rob a bank. It's because it's where the money is. Well,

the electric grid is not a bank like financial services, but we have a lot of value and we're certainly seeing a large rise in cyber crime. And it manifests itself probably in two different ways. One is the stealing of customer information, credit cards, other things. The other would be this new wave of ransomware that we're seeing. You're all are very familiar with the Wannacry problem that we saw globally about a month or so ago.

Again, that area, that theft of information and theft of value as well as reputational theft, those are all things we can understand. We can mitigate. It's a nuisance problem. But where we get into the stuff that really worries us with the grid is that folks are able to cross a boundary and begin to manipulate control systems. That is the growing concern area. It's largely been theoretical, but we've seen through the Ukraine incidents and others that the theory is now becoming practical and our adversaries are very interested in some of the successes that they've seen.

We've done quite a bit of studies and have released a number of white papers and have worked very closely with others in our sector, many who are sitting here, as well as other industries to better understand and analyze what's going on. The worst case, of which we've got very few examples, is beyond just disruptive like what we've seen in the Ukraine, but destructive where you have an

adversary get in and actually break things, either logical destruction causing the devices where they can't respond to commands or physical destruction, such as spending device, which the (0:04:37.1) Group had uncovered with Aurora many years ago. I don't want to say that's right around the corner, but that seems to be the next wave and that's where we really need to be vigilant when it comes to cybersecurity.

So I've got quite a few remarks in my written testimony. I encourage conversation and questions. Look forward to a vivid discussion as we move forward. Thank you very much for the opportunity to be here today.

MR. BARDEE: Thank you, Marcus. Next, we have Dr. Manimarun Govindersu, from Iowa State University.

STATEMENT OF DR. MAINARUN GOVINDERSU

DR. GOVINDERSU: Good afternoon. First of all, I express my sincere thanks to the Commission for providing me this great opportunity to be part of this panel. I'm a professor at Iowa State University. I conduct research in cybersecurity for the electric power grid.

As you know, modern grid is a complex cyber physical system with incorporation of smart sensors, communication networks, various controllers. They've improved. They appreciate the availability and the economics of the grid, but they're also increased the

attacks and risks of the grid for adversaries to exploit, so we need to secure those attacks and risks. We need minimize the attacks and risks.

So in recent years, the cyber threats have been growing in numbers, also in sophistication. We know of several incidents in recent years in the Ukraine and other places. The legacy nature of the grid, coupled with the slower adoption of operation technologies makes this problem even harder.

So in this context, I would like to identify a few R&D challenges and also they are related to policy as well. One important thing is we need a holistic cybersecurity framework that encompasses attack, deterrence, prevention, detection, mitigation, resiliency and forensics. We need to have a holistic as opposed to a comprehensive framework. That also has to accompany with property at the realistic metrics and tools and they are to be operationalized and realistic environment.

The other important thing is risk assessment has been talked today. The current cyber assessment is more qualitative in nature as opposed to quantitative in nature. And also they do not properly account the threat tactics. If you look at risk assessment, risk involves threat times vulnerability times the consequence. Threat modeling is not well understood. It is more of an art than a science today,

so we need to better understand threats so that we have more realistic risk models for cyber threats.

The third important thing is the current notion of resiliency is a fault resiliency which has the notion of N minus one contingency criteria. How do we transform the current fault resiliency to attack resiliency to deal with malicious adversaries who target multiple critical elements -- coordinator attacks and so on. So paradigm shift from fault resiliency to attack resiliency is important.

The other one is the innovation in IT outpaces the operational technologies. There is always a catch up in OD trying to catch up the IT. The adversaries have advantage because they use IT tools and technologies. How do we bridge this gap is very important. NERC compliance has been very effective over the years. Continuous improvement is important. While we make this continuous improvement, it has to be to the extent very fine, the effectiveness of the process, the technologies, and the people who operate the system they all have to encompass what has been in place. The challenge has been how do we sustain it? The industries find it hard many times how to sustain this compliance process.

The other important thing is how do we extend supply compliance to distribution grid. Distribution grid is not well -- or well protected against cyber adversities.

That needs careful attention. Grid exercise has been growing in terms of industry participation and sophistication of the scenarios. There is a need to incorporate test-based experiments in grid exercise scenarios.

Finally, workforce development is extremely important. As I come from university, we imparted graduate education, undergraduate education, industrial training, hack-a-thon and so on. There are so many flavors of education that can happen in which industry, university, and federal agencies can collaborate together.

So finally, synergetic partnership among industry, universities, and federal-funded national labs is important, not only to advance the R&D in this important area, but also to educate and train skilled workforce in a sustainable manner for the future. That concludes my remarks. Thank you again.

MR. BARDEE: Thank you, Doctor. Next, we have Michael Assante from the Sampson Institute.

STATEMENT OF MR. MICHAEL ASSANTE

MR. ASSANTE: Good afternoon, Chairman LaFleur, Commissioner Honorable, and staff. I thank you for this opportunity. I'll summarize my remarks for brevity.

In addition to my experience as a CSO at AEP and the first CSO at NERC, I'm providing these comments based on

my recent experiences with real world incidents involving power systems and my understanding of the opportunities and challenges developing industry standards.

I remain steadfast in my belief that properly developed standards play an important role in establishing a very strong foundation for future electric system reliability and security. It is important, however, to recognize that the standards cannot be formulated to fully protect against all possible manifestations of future cyber intrusion and attack.

The NERC standards have grown considerably in both scope and effectiveness over their 14-year history. While much has been done, there remains much to do. There will always be a regulatory lag between the CIP standards and current cyber threats. Acknowledging this lag, there should be a focus to enhance emergency operations and incident response requirements.

In this way, even if the standards do not specifically require a control or mitigation for unknown attacks of the future, the standard would still provide guidance to facilitate a response and recovery. For these reasons I believe additional modifications to CIP008 and CIP009 should be a priority for industry consideration. For example, required communication with the EISAC upon identification of a potentially impactful incident rather

than upon an actual impact to a reliability service would provide earlier visibility in an effort to protect other utilities.

The requirements as they are today would be comparable to a medical professional not sharing the results of your routine medical tests or cancer pre-screening for your awareness and early action, but instead waiting until you had organ failure to alert you that you have Stage 4 cancer. The requirement is written at such a high bar that few conclusions can be made or taken from the lack of reports that we see.

Also, we need to learn from other NERC reliability standards. I believe the standards need to mature in three ways. One, require a similar level of competency demonstration for the cyber defenders or cyber operators, if you will, at the Bulk Electric System. Two, acquire a level of response knowledge and capability of the certified electric systems operators, ensuring an understanding of appropriate responses to their systems being misused. And three, develop the operating protocols, tools, and capabilities to rapidly ascertain the risk of continuing to operate parts of the system containing attacks and developing approaches to measure the integrity of systems if they're being returned to service.

There are many lessons to be learned stemming

from the 2015 and '16 Ukraine incidents. We need to move beyond the question of whether similar attacks is possible in the United States and instead shift our focus to mitigation and response requirements with the expectation that a similar or even more impactful attack could occur here. Continued efforts from NERC focused on utility exercises like Grid-x and Dewey-lead industry workshops and private sector provided technical hands-on training will continue to improve our overall capabilities and preparedness.

This is a very encouraging area where I believe NERC registered entities are moving far beyond the requirements in the standards. Recently published reports examining the 2016 Ukraine cyber attacks targeting their country-wide transmission system operator, paint a picture of an evolving threat. Analysis of the malware describes a tailored tool for the purpose of causing electrical outages. The flexible and modular tool possesses features that aid the time in collapsing the time it takes to complete the necessary steps to device and launch an attack that can disrupt operations and potentially damage infrastructure assets.

Also, it appears that the attacker interest in system protection has moved from information gathering to developing an initial capability to exploit both control and

protection. Threats like this demonstrate that we must empower defenders with defensible environments, which the standards do. To this end, though, industry also must have the latitude to experiment and field new prognostic and security technologies that can change the pace to catch up to cyber attackers.

As an example, the Idaho National Laboratory and industry partners are further building upon the industry's great strength by developing engineering-centric assessments and mitigation methods called Consequence Driven Cyber Informed Engineering. The goal of this program is to actually engineer out the worst cyber risk that the energy infrastructure faces.

Finally, public reports of successful broad axis campaigns and modular toolkits may indicate attackers are becoming more focused on attacking larger numbers of devices to cause widespread impacts. The positive evolution of CIP standards have provided more protections to a greater number of systems and this may need to continue.

So with that, I thank the Commission and staff and look forward to our discussions.

MR. BARDEE: Thank you, Mike. Next, we have Greg Ford from the Georgia Systems Operations.

STATEMENT OF MR. GREGORY FORD

MR. FORD: Good afternoon Madame Chair,

Commissioner Honorable. I appreciate the opportunity to participate on the panel on behalf of NRECA and our member cooperatives in Georgia. There are no single standard requirement that stands out as the most effective cybersecurity control. Instead, I believe it is the interrelated nature of the controls that together provide a defense in depth posture that makes the NERC CIP standards effective.

The key aspects of CIP Version 5 was the introduction of the cyber system impact categorization, which has expanded protection to the entire Bulk Electric System while acknowledging that not all facilities have the same risk profile. While I have noted that standards work together as a whole, it is important to point out that Version 5 introduced controls that are consistent with a key lesson learned from the Ukraine event. CIP Version 5 requires that all interactive remote access first pass through an intermediate system and leverage multifactor authentication.

In addition the CIP standards, internal controls that the industry is adopting ensure compliance and more aggressively mitigate security risks. We have internal controls not only for CIP operations, but also for other Bulk Electric System operations. We have embraced internal controls as a part of our day-to-day operations to help

avoid mistakes and prevent cybersecurity breaches. At GSOC, board-approved corporate goals measuring the implementation and testing of these internal controls are a component of our employees performance pay.

We urge restraint on pursuing new mandatory CIP standards. We are still in the first year of CIP Version 5 and have not yet completed the implementation of some requirements for low impact systems. Time is still needed to fully implement these standards and absorb the lessons learned from this implementation.

Further, we need to avoid thinking that mandatory standards are the only path to improve security. We believe that voluntary recommendations and actions should lead before the mandatory standards because they are faster to implement and more flexible to change. Organizations such as the EISAC are well positioned to coordinate voluntary recommendations to the industry.

We also recognize that as the cybersecurity field continues to mature new technologies will be introduced that could improve the overall security posture of the grid. These new advanced security technologies will no doubt come and go. By the time the new technology can be incorporated into a mandatory standard, it may no longer represent the state-of-the-art. The approach moving forward must ensure that a solid security framework is in place, but

also enable us to be nimble in the face of an ever-changing threat of our landscape.

During the first year of mandatory compliance, we learned that some standards are taking a disproportionate amount of time to execute. In particular, we highlight CIP 7 and CIP 10 baseline standards. While we certainly recognize these standards are important, we believe that improved security could be achieved if they focused on having adequate controls in place to achieve the security objective rather than specifying performance details.

For instance, the current patching requirement dictates a specific process across all devices to assess and implement security patches within a detailed timeline. An alternative approach could be to focus on the security objective of implementing a flaw remediation and vulnerability management program with the flexibility to recognize different areas of risk and apply resources accordingly.

As our industry expands a culture of internal controls, we need to continue to move towards an environment where the focus of the oversight is on ensuring that controls are in place to monitor and maintain compliance and security. In this environment, deficiencies that are detected and corrected by a company's control should not result in a violation.

The Electric Subsector Coordinating Council is a key coordination point between the electric sector, the government, and other critical infrastructure, such as telecommunications, oil, natural gas, financial services, transportation, and water. The ESCC is working coordination with the EISAC to bring these sectors together to improve cross-sector awareness and facilitate cross-sector exercises. The upcoming Grid-X4 exercise is just one example of how the electric sector is committed to improving the resiliency and ensuring cyber preparedness.

In conclusion, we appreciate the focus and the effort of the Commission to improve the security posture of the grid. The existing CIP standards mandate that necessary elements of a solid foundation cybersecurity program and have contributed significantly to the improved security of our system.

I'd like to thank the Commission for the opportunity to participate on the panel and I look forward to questions. Thank you.

MR. BARDEE: Thank you, Greg. Next, we have David Ball from AEP.

STATEMENT OF MR. DAVID BALL

MR. BALL: Good afternoon. On behalf of AEP, I'd like to thank the FERC Commission and staff for the opportunity to speak on this topic.

AEP applauds the efforts of the Federal Energy Regulatory Commission in assembling this technical conference on a topic so crucial to the reliability of our nation's electric grid. AEP is one the nation's largest electric utilities delivering electricity and customer energy solutions to nearly 4.5 million customers in 11 states.

AEP owns the nation's largest electric transmission system with more than 40,000 miles of network transmission facilities. We operate 224,000 miles of distribution lines and rank among the nation's largest electric generators with 26,000 megawatts of capacity, which includes 3200 megawatts of renewable energy.

Cybersecurity, like all security, issues is of paramount importance at American Electric Power. We have a robust cybersecurity program at AEP, one that is under continual evaluation for process improvements. We are in constant contact with our state and federal regulators and our regional reliability entities to ensure that we are current on all threats that face us so we can institute the best possible protections.

AEP would like to thank FERC and NERC for the standards created and enforced in the area of cybersecurity. The standards serve as a starting point help drive a common framework for the cyber and physical security protections in

which AEP engages. The checklist of NERC standards is a solid foundation, but if we were to engage in those activities and nothing more our Bulk Electric System could be seriously at risk.

AEP engages in many voluntary actions to improve both the overall cyber and physical security of our system that is part of our large Bulk Power System. These are precautions and protections we implement because they are the right thing to do.

You asked about specific protections and asked us to relate our practices to internal crisis that have arisen in the past few years, most specifically, the attacks on the Ukraine electric grid. Speaking to the 2015 Ukraine cyber attack, security regulations already in place in this country would prevent such an attack from occurring here. The attackers in the Ukraine incident infiltrated the cyber systems and observed work patterns and practices for months before seizing control of the Ukraine grid. Their efforts were enabled by the fact that the business systems and operations systems were integrated. This mixing of functions violates U.S. regulations.

Because our systems are separate, an attacker could not hack into the business functions of U.S. grid operations as a means of access to operational systems. For example, standards for patching, configuration, change

management, and malicious code prevention have driven industry to implement a framework of controls to protect our critical system from vulnerabilities and exposure to cyber attacks such as Wannacry attack in May of this year.

The CIP standards also have helped in restricting communications in and out of our SCADA networks, which we saw exploited in Ukraine in 2015. Also, we require intermittent systems and multifactor authentication to ensure only authorized personnel and communications can access our SCADA network.

We need additional transparency and consistency in the auditing process. Currently, different regions view standards differently and we sometimes are challenged by those inconsistencies as we strive to meet the demands of three regional entities. Additionally, when problems are revealed during the auditing process those issues need to be transparently outlined in an audit report issued by the regional entity. Transparency and consistent terminology in communicating violations would greatly enhance the benefits of these audits.

Another area to consider related to consistency is our frequent standard revisions. This presents a risk as the resources needed to improve and maintain cybersecurity often are consumed with keeping compliance processes up-to-date to reflect standard revisions. For the past two

years, the industry has been advocating for increased screening processes for new hires in the cybersecurity arena. Currently, background checks are conducted by third-party vendors using publicly available data.

To increase security of the grid, we should be able to access fingerprint records housed at the Federal Bureau of Investigation. This would not necessarily need to be a standard practice for utility new hires, but could be restricted to those working in critical infrastructure and Bulk Power System positions. The industry would benefit greatly from the Commission's support in this endeavor.

In conclusion, I would like to reiterate that AEP is fully committed the security of the electric grid as discussed above, consistency and transparency and NERC requirements would help facilitate our compliance, support from the Commission as we advocate for FBI assistance in background checks of new employees would be helpful, and strong communication and relationships between the Commission and the states would be beneficial as we work to ensure the security of the grid.

Again, we appreciate the opportunity and I look forward to your questions.

MR. BARDEE: Thank you, David. Next, we have Nathan Mitchell from APPA.

STATEMENT OF NATHAN MITCHELL

MR. MITCHELL: Thank you. I want to thank the Commissioners and FERC staff for inviting me to participate in this technical conference on grid security. I am here representing the over 2,000 municipal and state-owned electric utilities that make up public power.

I would like to remind the Commission that APPA and its member utilities have supported the work of the industry-led standard drafting teams in their efforts to develop risk-based standards through the NERC standard development process. These standards provide a needed baseline of cybersecurity controls to protect the Bulk Electric System; however, we cannot continue to write new standards to address every threat. APPA believes that the CIP standards need to reach a steady state.

We are encouraged by FERC staff's recent request for input on how standards can be made more efficient while maintaining their effectiveness. APPA stands ready to assist the Commission with its request to right size the standards to make them less burdensome on industry.

Please don't take my suggestion as an indication that we should not continue to protect our system from ever-increasing cyber threats. I believe that more can and should be done to address the cyber risks to electric utilities, but these efforts should be focused on voluntary programs outside of the NERC standard development process.

I would like to highlight one voluntary program being developed to help public power utilities address cyber risks.

As I provide a description of these efforts, the Commission should recognize that it meshes with other industry, government, and university efforts discussed by my follow panelists and to make up a community approach to cybersecurity. APPS has partnered with the Department of Energy to undertake an extensive, multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities.

In this project, APPA is providing public power utilities with an array of security tools, technologies, and programs so that the community is better able to understand, install, and implement new cybersecurity programs. Importantly, this project will bolster the programs for many small utilities that do not own or operate bulk electric system assets and thereby, not registered with NERC.

First, we have developed a simplified maturity model as a tool for small utilities to understand the characteristics of a mature cybersecurity program. The maturity model will help public power utilities enhance their cybersecurity program based on their organizational structure risk profile. The project has begun to evaluate information-sharing tools and technologies that will improve

threat information sharing between utilities and the EISAC. Recommendations will be developed on how best to characterize, assess, disclose, and disseminate secure threat information that is useful and useable for public power utilities.

And I believe that workforce development is essential to ensuring that public power utilities have the proper human resources to manage their cybersecurity programs. Public power utilities often face difficulties in identifying and recruiting qualified cyber and physical security candidates due to their location and/or size. Working with universities, community colleges, and other educational and training institutions across the nation, we will explore the development of educational programs that meet the staffing needs of a typical public power utility. We will then evaluate if online opportunities can be developed so that they can be easily accessible to remote communities.

I look forward to the comments of the other panelists on how we can educate our current and future workforce to address these cybersecurity challenges.

Finally, the industry needs a robust cyber incident response plan. APPA plans to develop a model playbook which will address potential roles and responsibilities within small public power utility to

respond to a security incident. In many small utilities, one person has many roles and responsibilities. As such, a step-by-step playbook on what actions to take first, who to coordinate with, and other types of response activities will supplement existing natural disaster mutual aid programs.

I refer the Commission to the other industry incident response playbooks, such as the one created by the Electricity Subsector Coordinating Council, as a model for the public/private partnership needed to respond to a national level event. I believe that APPA's voluntary cybersecurity program will help improve the overall cybersecurity posture of public power utilities and the Bulk Power System.

I appreciate the opportunity to provide these comments and look forward to your questions.

MR. BARDEE: Thank you, Nathan. Next, we have Commissioner Robert Scott from the New Hampshire PUC.

STATEMENT OF COMMISSIONER ROBERT SCOTT

COMMISSIONER SCOTT: Thank you. And Chair LaFleur and Commissioner Honorable and staff, I appreciate the opportunity to speak. It's always good to see you again.

I speak today as a Commissioner for the New Hampshire Public Utilities Commission. In one week, I will be the Commissioner for the Department of Environmental

Services for New Hampshire; however, I want to make sure that the Commission is aware, recognizing the importance of the work that's been going in New England. The governor's asked me to also act as the special advisor on critical infrastructure for cybersecurity, so in the context of no good deed goes unpunished, I get to do that work also. So in that context, I hope to still be able to engage with you and your staff.

Again, speaking as a state regulator, I also wanted to thank you for allowing and bringing the state perspective to this panel also. I think that's an important one. And I'll state the obvious, at least from my point of view. Obviously, the Bulk Electric System is very important to us all. However, as I'm sure you're aware, that the distribution systems also present a threat to the Bulk Electric System, so we need to work together in that capacity. Or to put it another way, obviously, NERC and FERC regulate the wholesale side of things, but unless the state regulators are involved in an effective way and the distribution utilities are involved in an effective ay I don't think we get where we need to go. Certainly, any artificial boundary like that is not going to be recognized by the adversaries that we're looking at for cybersecurity.

Our experience in New England demonstrates this interdependence. What we found is in working with our

partnerships that we've developed cybersecurity for our largest distribution utilities and the transmission owners are basically one in the same, so they're centrally managed, rightly so. It's generally the same staff and the same systems, so it's very hard, at least in New England, which I don't think is that unique to differentiate the two nor should there be.

In that context, I have some recommendations to point to, based on our efforts in New England. First and foremost, is the important of partnerships, we partner with the National Guard in the region, with the Department of Homeland Security, particular, the INA side of DHS. Certainly, FERC, the Office of Energy infrastructure Security has been a great asset for all the states, ISO New England, and to a lesser extent the FBI and Department of Energy.

I'll highlight. We've talked in your supplemental notice and some of the other panelists have talked about the Ukraine incidents that are going on, which are very concerning. Another incident which raise light in New England and thankfully it wasn't -- I don't want to say it wasn't real, but it was over -- incorrectly reported it was Burlington Electric situation.

That highlighted to me anyways as a state regulator the importance of those partnerships and the

importance of having relationships already. So we had in that situation -- I'm not going to characterize it as good or bad, but we had a governor make some very strong statements. So the governors need to know what to say and what's going on. I know, for me, I received a call. I was shopping Saturday morning and I got a call from the governor's office what's going on. And thankfully because we have these partnerships I was able to say I've already been in contact with these people. They're on the phone now with EISAC and yes, it's all under control. We're good to go. Those things are important to states.

So the other part of that, and again the Burlington Electric incident provided a good insight for the need of this is we need to exercise these things. So again, FERC, OEIS has developed some checklists that helped with the states in New England that we've been looking at. That has now set us up so that we can now start to conduct some exercises. So again, you don't know what you don't know until you start going through these types of scenarios.

Last week, with the National Guard, we had state regulators. FERC had staff there. New England Utilities, ISO New England were all participating in the New England National Guard Cyber Yankee Event, so that was yet another way you taking it to the next level of working together and understanding each other.

Another point I'd like to raise is security clearances. As the Commission's aware, a few years ago New England was in a very unique position as we had three state commissioners from three different states, myself included, with top secret or above clearances and we knew how to spell the word "cyber." So in that context, we were able to have discussions with the intelligence community, with our partners in Kansas, among others, as well as to start to talk to our utilities on the importance of collaborating on a classified level.

That resulted in New England of we've actually hosted in New Hampshire. We've been able to host a meeting of those obviously appropriately cleared to bring utilities and regulators in so that they could share information with each other, talk about common experiences at that level. That's something they haven't really been able to do in the past with that. Also, this experience has also allowed us to start to work to get higher level clearances for appropriate utilities, so we feel that's an important consideration moving forward.

Workforce development, again, New England's been taking a regional approach, understanding that we're all interconnected, especially in New England. The State of Maine, as part of our regional effort, is actually hiring a gentleman July 3 who was working with Cyber Command. He's

retiring. He has the credentials and clearance, et cetera. He'll be working certainly as a State of Maine employee, but he'll also be a regional asset to our efforts.

Having said that, that's kind of a work around what I think the Commission surely understand. At the state level, we're generally not staffed for these types of things. We don't have the expertise. We have accountants. You know we're here to be -- regulators and this is a new ground for us. So NARUC's done some groundwork, which has been very helpful, but that's something else that continues to need -- I think will need help because I don't believe this issue is going away.

Finally, again, I want to put a shout out to the FERC Office of Information Security -- Office of Energy Infrastructure Security. They've been a really great resource for our states and if we've called they've been very responsive to us, so I want to throw that out as a best practice. Perhaps other agencies could do the same.

So with that, I'll close my remarks.

MR. BARDEE: Thank you, Commissioner. And Brandon Wales from DHS.

STATEMENT OF BRANDON WALES

MR. WALES: Thank you. Good afternoon, Madame Chair, Commissioner Honorable and assembled staff. Thank you for the opportunity to address you today on behalf of

the Department of Homeland Security National Protection and Program Directorate.

MPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. And within MPPD, I oversee the Office of Cyber and Infrastructure Analysis, whose mission is to provide analytic support to our collective efforts to strengthen the security and resilience of our infrastructure and respond and recover from natural hazards and manmade events.

My testimony today will focus on two issues of interest in response to the questions posed to the panel. The first issue covers the need for traditional electrical utility planning activities to embrace cyber-base contingencies and the second issue focuses on the efforts of the Department of Homeland Security to increase and enhance information sharing and analysis activities with the electric sector.

First, as electric utilities adapt and increase their use of industrial control systems to automate and increase the efficiency of operations, cyber-related consequences of adoption of new practices and procedures should be carefully studied and evaluated to understand the potential impact of their loss or disruption to reliable operation of the electrical grid.

Cyber hazards do not have as well characterized likelihood and consequences to critical infrastructure assets and systems and cyber events can simultaneously occur over large geographic areas without respect to traditional boundaries of electric system operation or control. These events will stress traditional emergency management and response procedures designed to contain and constrain system problems.

To understand potential system impacts, a natural evolution may be for system planners to create a number of cyber contingency cases which could incorporate a variety of cyber threats that could affect system monitoring or communications and affect infrastructure operations. Cyber scenarios should have characteristics distinct from current hazards to challenges the utility's understanding of the degree of the impact possible from cyber events.

Second, the Department of Homeland Security works with partners at all levels of government and from the private and nonprofit sectors to share information and build greater trust to make our cyber and physical infrastructures more secure. This includes sharing information through platforms such as the Critical Infrastructure Advisory Council, the Electric Subsector Coordinating Council, and the Department's Physical and Cybersecurity Operation Centers, the National Infrastructure Coordinating Center,

the NIC, and the National Cybersecurity and Communications Integration Center, the NCSCIC. Information released by the NCSCIC and NIC maybe subsequently shared to the electric subsectors, owners, and operators through the Electricity Information Sharing and Analysis Center.

One of DHS's most prominent initiatives to enhance information sharing between the federal government and private sector that I would like to highlight is called Automated Indicator Sharing. AIS connects participating organizations to a DHS management system at the INCIC that allows bidirectional sharing of cyber threat indicators, helping to build the common, shared knowledge of current cyber threats.

AIS is a part of the Department's efforts to create an ecosystem where as soon as a company or federal agency observes an attempted compromise the indicator will be shared in real time with all of our partners, enabling them to protect themselves from that threat. This means adversaries can only use an attack once, increasing their costs, and ultimately reducing the prevalence of such attacks.

Another initiative to facilitate information sharing is the Cyber Information Sharing and Collaboration Program, which enables the sharing of cybersecurity threat information in a secure fashion with entities across

critical infrastructure sectors. CISCP, as it is called, provides for analytic collaboration between DHS and participating entities, and when appropriate, allows participating entities to embed analysts on INCIC watch floor. These efforts are designed to feed and complement energy sector initiatives that were highlighted in Mark Sachs' written testimony.

Future cyber events may not directly target electric power owners and operators, but may impact connected infrastructure systems, which the Bulk Electric System depends to ensure reliable operations. As our information technology systems become further interconnected and interwoven, disruptions will no longer be limited to a single infrastructure asset or system with consequences potentially far-reaching.

The issues I have raised here today are complex and don't lend themselves to the easy, silver bullet solutions. The Department of Homeland Security is committed to working with FERC and our partners in the electric sector to begin working these and other challenges facing the systems that power our country.

Thank you and I look forward to your questions.

MR. BARDEE: Thank you, Brandon. We'll start our questioning with Commissioner Honorable.

COMMISSIONER HONORABLE: Thank you, Mike, and

thank you gentlemen for your perspectives. I have a lot of ground I'd like to cover, but first I'd like to start by thanking each of you for the value you bring to this important work and I think we end it on an important note about focusing on the importance of this work and how much more challenging it was.

I remember, and I've been hearkening back to my state regulator days, but I remember we had a physical attack on our grid and that was my first encounter with the Joint Terrorism Taskforce and the friends that we have at the Department of Homeland Security thank you for your work. And I was able when I NARUC president to participate on the Electric Subsector Coordinating Council.

Also, Brandon, your colleague, John McClain sends me your daily updates, so thank you. I am well informed about the world of cyber, but it's a shame the state of affairs these days requires that, but it absolutely -- going back to Marcus's point, requires our vigilance that we're aware and that we're equipping ourselves with the tools to lead and to lead well.

Bob, I mentioned earlier today for our work with our state colleague, thank you. And I recall when I signed up to be a Commissioner, and I know it's the same for you; you had no idea about all of this part of it. And now you're going over -- thank you for your service -- to

another job and the governor's managed somehow to get you to do both at the same time. Thank you for saying yes because this work is so important. And men and women who have your experience and expertise are few and fair between, so thank you for saying yes. Your state colleague, the region will benefit, but also we will as well. So thank you for coming back for more.

I'm really pleased to end with this session because I think your perspectives have really covered the gamut of the fact that we are all working so hard on a number of aspects of grid security.

And I want to start with, Marcus, you talked about -- and thank you for your discussion about the threats and how different they are and it's important that we not lump all of them into one. We tend to talk about cyber generally when there are a number of aspects about that work that we need a singular focus.

But you spoke about ransomeware and disruptive threats. I wanted to focus on the crash override malware because you all recommended steps that utilities need to take to protect themselves and I appreciate your work along with DOE and our Office of Energy Infrastructure Security to really study what occurred in Ukraine to make sure it doesn't happen it here, and if we do have a threat or an attack, how we can quickly rebound. And I want to ask you

to just highlight some of the challenges that were presented by this malware and the strategies that we can employ to fend against that.

MR. SACHS: Thank you, Commissioner. That malware was interesting. First, we were not aware of it in the United States until a Friday and others were aware of it maybe two or three weeks earlier and it was not something widely known by any means. But do a good, strong public/private partnership on a Friday afternoon many of us working the weekend were able to get information out on Monday morning.

The group that discovered it in Europe had already planned to do a release to the media on their own. That group found a group in the United States, another private sector organization. They asked them would just please review what we're doing to make sure we're not saying anything technically wrong. That U.S. group said, well, if you're going to go live in the media, we need to activate. You know put up the bat sign to get people involved, so it was a very strong effort that just came together because the partnerships were in place. That if we didn't have those partnerships already existing, we would've failed that weekend and you would've had a media splash on Monday morning that none of us would've been ready for.

So the malware itself I don't know that we

necessarily need to focus on the ones and zeros of the malware.

COMMISSIONER HONORABLE: We don't. I just want to get your takeaways about it.

MR. SACHS: Absolutely. And I think there's so much more to learn about our adversaries. So when this malware was found, it is showing us new techniques, tactics, and procedures, or TTPs that again are long and theoretical, but now we're actually seeing it in software where an adversary who can build a modular tool, as we like to call it. It's almost like a Swiss Army knife. You've heard that analogy used.

COMMISSIONER HONORABLE: Yes.

MR. SACHS: Where this thing can be customized for different types of targets. It can lie resident undetected. It looks like regular software, but yet, it has a little evil bit to it. So instead of looking for signature, which is our typical way of looking for it, strings, ones and zeros, IP addresses, we now need to look more for behavior-based signatures. Things that aren't working like they're supposed to, which then requires a much deeper knowledge of what is it supposed to be doing, what is baseline, what is normal, and then being able to recognize what is not normal and then quickly determining is that a human error causing it to be not normal or is it something

we don't understand, which then they say, oh, we have a cyber problem going on.

And so this is going to require again another level of thinking versus just looking for signatures and malicious code, which is what we've really been doing a lot of and we're getting good at it, but it doesn't stop there. Again, I was thinking about agility. We have to keep rethinking how we think about security.

COMMISSIONER HONORABLE: Indeed. I don't know if anyone else wants to chime on that point, but if not, I will move onto the next one.

In thinking about your point about the partnerships, and it's similar to what Bob Scott mentioned about the call he got and because of his networks he was able to respond quickly about what was occurring, I want to emphasize the global nature of this work. Thank you for mentioning that.

I often say energy is global. That's why our work and why we invite our international colleagues here. We're working on the same issues. We're working on the same challenges and in particular in the grid security space, in the cyber space that's especially important. So I thank you for cultivating and nurturing that climate.

And to Bob Scott's point about lessons learned about that Burlington incident, I wanted to say that, yes,

we learned the importance of being prepared to respond, as Marcus just mentioned, being prepared with what we need to say in the media and what we don't. But another thing is something you mentioned and that's ensuring that we have a strong partnership. And I think, honestly, and I'll say it, for our part in the federal government we had some missteps too in that incident. And I think we can all learn from that and our goal should be inspire and strive for trust and for our ability to work well at all times. So I appreciate that you were candid about your takeaway. I want to be candid about us too, so we'll have to learn to trust and protect when industry provides us with information voluntarily that we keep it, as we should and as we've promised.

I want to turn also to the workforce question. Greg Scott and Mr. Ball thank you both because you've talked about workforce strategies.

Greg, you spoke about performance-based metrics with compensation. Hello, that gets everybody's attention. You start messing with my money, then I'm going to pay attention and what the hoops I have to jump through. That's important. And I want to ask others if you have grid security related performance metrics in your places of work, so think about that.

But also, David Ball mentioned your workforce

component as well and I want to tell you both how much I appreciate that. It's more than just us going to meetings and giving speeches and hearing lectures and reading studies. This is about making sure our men and women are trained because we're only as safe as the weakest link. That applies to our facilities and it applies to manpower too, so I was very pleased about staff's question for you. What can the Commission do to facilitate or encourage a strong cyber workforce?

I think about that internally. What are we doing to make sure that our staff is trained? We have trainings that focus on not clicking through on that darn thing we know we don't need to click on? What does that also elate to with regard to hiring the best? That's a great story about Maine snagging the gentleman that's retiring. Those folks are few and far between as well.

How can we ensure in the same way that we're hiring the best market operators, transmission planners, that we're hiring skilled people who are equipped to help us secure the grid? So two questions, one is about your strategies where you are about making sure that grid security is a priority and then what are you focused on externally for hiring talent.

And I think we're getting feedback, so if you aren't speaking, please turn off your microphone. Thank

you.

MR. FORD: Thank you, Commissioner Honorable, for that acknowledgement on our performance and how we handle things. When we started with this route 10 years ago, of course, security and reliability is important to us all. It was very important to us as we saw this culture changing we wanted to try to get ahead of it and we felt like there was no better way to get people's attention and get the culture in the right frame of mind in putting performance pay type of activities in that loop.

So every year we have always had measures or metrics that were related to performance pay. And when you're talking about changing to the culture of cybersecurity years ago -- 10 years ago, I'll be the first to admit cybersecurity to me was getting my antivirus updated on my computer and that was it. Today it really consists of various things, starting, one, with your people. You have to train. You have to make them aware of things. You have to continue to hit those exercises to get them to the right behavior that you want, phishing exercises, for example. Don't just do one phishing exercise a year. Do 10, 15, every how many it takes to get that culture to start looking at those external emails differently and not clicking on links.

Processes, the standards are a big part of that

and our internal controls. Now we know and have knowledge of our inventory. We have controls around protecting those assets. We're concerned about the isolation factor of whether we're using data diodes or physical air gaps, whatever the case may be. We have patching processes. All of these things change the culture to help us look for these malware detections and intrusion detections.

And lastly, is our technology and I think we're now moving into that phase of our process, which is making sure our vendors give us good, high quality technology of our computer systems so that we can bring all this together as one business unit to support our system. So we've been doing it for a while that way. As far as our performance, it was geared towards changing that culture. From the building and workforce perspective or question, that is always a tough one because the electric utility 30 years ago was the place to go to out of college. Today it's harder and harder to pull those college students, so we're always looking for ways that we can help encourage that.

Once we have them in place, the Department of Energy, Department of Homeland Security, Department of Defense, they have very good, knowledgeable people at getting training. The industry can learn from getting training from those organizations as well. I would ask for the Commission consider helping us foster that along even

further than what we've done.

COMMISSIONER HONORABLE: Thank you. And I hope we'll accept that challenge because we do a terrific job, if I might say so, of working with our state colleagues, with industry. If I go out on a tour of a construction site and if I see something that's maybe not quite right -- I'm not an expert, but I might kindly say would you all be open to an architectural review? I might mention it to Joe and to Dave and we've really fostered some great relationships that way. It's not a "gotcha" exercise. It's our way of really helping to strengthen your physical security, your infrastructure, your grid security and so it helps us all.

So I think you're right in that we can always find new opportunities to support the work that you're doing. And we, too, are challenged with that. We happen to rank really high for attracting millennial to our agency and we're proud of that. But then, some of you guys like to pick them off after a few years, so it's an ever-evolving thing for us.

Is there anyone else that has a comment? Yes?

MR. BALL: In our written testimony, we referred to hybrid skill sets in cybersecurity and this may be something that Michael can expand a little bit on as well, but it's easier to find individuals who are familiar with cybersecurity when it comes to traditional IT and

Windows-based infrastructure. The more difficult skill set to find today is individuals who have a power systems background who is familiar with the OT technology and understands what it means to build cybersecurity into the OT network. And for us, inside of AP, that would be our SCADA network.

COMMISSIONER HONORABLE: Commissioner Scott?

COMMISSIONER SCOTT: Again, from the microcosm of New England, I just did some math here. Out of the five major utilities that we've been working with in the past four months there's been four staff changeovers. You know four key people that we were working with say, okay, I'm leaving. And the good news is the utilities are committed to this, so they're able to say, okay, here's the person who's going to replace them. But again, I'm not sure, but my guess is when you have people of these types of skills are very marketable and they're very mobile.

Having said the obvious, and you've worked at a commission at the state level, we can't hope to attract with other people. And I mentioned the Maine experience. That was the stars aligning just right, so you had a gentleman who is not for the money. He wants to relocate to a certain area. He has a retirement, so we're able to capitalize on that, but that's a big challenge for the states. We can't attract and retain the people with those types of skills.

COMMISSIONER HONORABLE: And I appreciate that. And honestly, I'll admit this; I've called people and said enough. You've taken enough of our people after the third swipe. One of them may be sitting in the room today, so I won't say the entity, but I did call and say enough already now. We've got work to do too. Leave us some of our good people. But it is a challenge for us and this isn't a fluff issue for me.

When I came to FERC, 40 percent of the energy sector was eligible for retirement. When you think about this most important function of ensuring it's security and it's safe, and I just said it in a speech a couple of days ago, what's the point of having affordable, diverse energy if it's not safe and secure. And so the work that you're doing and our efforts to attract people to carry it out is key. And I'm preaching to the choir, but I appreciate that you've taking the time to share your experiences. Anyone else?

MR. ASSANTE: I would just add that coming from a training organization it's important to note that power utilities are the leading sector in industrial and infrastructure area training their staff, and the training goes to the place where we've seen automation professionals, power engineers, even dispatchers receiving cybersecurity training in order to understand that in lead teams. So

we've definitely seen that from the electric sector.

I do think the standards and the awareness and the industry's understanding of its importance to reliability has driven that. And I would say that the grid exercises is also an incredible forum which has brought both the engineering disciplines and the IT support and OT ICS/SCADAS support groups together to deal with multi-facet scenarios.

And in my testimony where I called for having to deal with things like operating protocols, one of the things that Ukraine taught me for sure was that the attack was absolutely structured in 2015 against the dispatchers. They lost the UPs and lighting and their phones in their own control centers and it was very clear that understanding that. And I do believe the grid exercise platform has been an incredible to industry and government partnership in order to be able to accomplish some of that learning, understand it, digest it, and develop the protocols that we'll need to deal with these types of things.

COMMISSIONER HONORABLE: I often say there but by the grace of God we go, and so we have the benefit of learning from that and employing it in our operation centers.

MR. SACHS: Let me just make two quick points. One is that this is fortunately not a new problem. I can

recall as early as 1999 when the Defense Department was first wrestling with what do we do about cybersecurity outside of the classified world, that one of the questions brought up immediately was what do we do about SCADA and so the term was in popular use almost 20 years. And we knew that there was growing issue and we knew there was a workforce problem.

This may have been talked about, this Grid-X thing that we do every couple years I think is so unique to us, but we're also seeing in the educational world a growing number of colleges, universities, and even high schools that are doing security-type exercises. And we're seeing this begin to grow almost organically, almost like sports, soccer, baseball, other things, very competitive.

This is good news and it's something we need to leverage and enhance and really kind of make it an all American thing that getting involved in cybersecurity as a career field early is absolutely what we want these young kids to do. Don't wait until you're 30 or 40 to discover cybersecurity, but discover it when you're 13 or 14 and really just dive into it.

COMMISSIONER HONORABLE: All I can say to that is Amen. And I spoke at an event in Houston maybe last year and an eight-year-old asked me about cybersecurity and it blew my away, but I thought kudos to you guys. I mean

someone has been talking about in a way that got the interest of an eight-year-old and that's what we need, so I couldn't agree with you more, and I won't say another word after that.

MR. GOVINDARASU: Just a quick comment, I think these are excellent points. As you know, the cybersecurity for the grid is an interdisciplinary field. We need to educate engineers, our future students who are featured in -- bringing both the cyber and physical flavor. I think a lot of universities have education program in cyber physical security for the grid funded by DOE, National Science Foundation, and so on.

As part of an effort, there are also hack-a-thon, cyber difference competition creating markup similar to the grid exercise. Those things are happening. Those are very well-established efforts. But the critical thing for both things to be successful is industry/university partnership. Universities they do things well with the education, but they need to understand the real, practical scenarios and those partnerships need to be center, but there is a lot more to happen.

That may not only be a training feature engineers, but also the current engineers who are in the field they could take certificate courses or graduate courses or cybersecurity training sessions like grid

security conferences and so on. So the universities have a critical role in workforce development, development in partnership with industry and other Federal Agencies. Thank you.

CHAIRMAN LA FLEUR: Well, thank you Collette. And thank you all very much. I want to especially thank Mr. Wales for coming over from the DHS. It's always important to have our government partners here.

A very interesting conversation, I was just looking behind me because my summer intern this summer, who was here for the morning session, but I think she's writing a speech, won some kind of hacking contest. I don't remember, first place in some Hack Princeton or Hack America or Hack-a-Thon, which I believe is just what you were talking about. You see they didn't have that when I was there since I don't even know what it's called.

I have a couple of questions. The first thing I want to talk about, Marcus, you mentioned in your pre-file testimony that there were new data sources to better understand the security landscape and Mr. Assante talked about -- I believe it was you, Michael, who said that the standards are too backward looking and we need more leading indicators of things.

Are there leading indicators of cybersecurity issues that we can develop? You know you've talked about

faint signals in other places. Some of the standards, I think, are intended to do that, intended to think if you're not careful about passwords you might not be careful about firewalls or air gaps or other things, but are there more cyber leading indicators we can look for in the system that will help?

MR. SACHS: We've certainly learned that cyber is not like a predictable system, so typically, when you do standards it's because you can predict a behavior. In Physics, you know like a railroad.

CHAIRMAN LA FLEUR: Like a safety pyramid, if you do so many of these you'll have so many of those.

MR. SACHS: Right. But security does have a baseline. There are some fundamental things that we all do. We call it hygiene. We call it best practices. That, of course, can be done, but where the adversary works is above that and the adversary doesn't care how compliant you are. Doesn't care which standards you've done. They don't care. They're just looking for ways to get in. So this goes back to then, well, how do find -- what are those faint signals? How can we see where the adversary is punching around looking for a way to get in?

You're familiar with our CRIP Program, the Cyber Risk Information Program? That generates an enormous amount of information about ourselves. We're able to look through

that information and find things -- as I was saying earlier, look for things that aren't normal, something new that's happened, something we can't explain and began to ask lots of questions. Some of the best analysts out there are those who are curiosity seekers. They just see something that doesn't look right and let's just start going down that road to see where it takes us. We may not uncover anything or we may uncover some brand new malware nobody's ever seen before, a new technique.

The information sharing, as Brandon mentioned of the AIS Program, we're embracing that. We're building out a pilot, so we're going to do the automatic information sharing. So again, if some entity sees something that's not right let the computer share that with other computers. The human tends to slow things down, but the human mind is something very special and can see things that are different. It can ask questions that a computer can't ask. A computer often doesn't ask why is something happening. It just says it is happening, but the human mind could say why and connect dots, as we like to say it.

So I think as we are getting better at understanding what security is, we're getting better at detecting when security events are happening and then getting better at analyzing them and asking that "Why" question so we can get the word out, so we can get others

involved. And always I'll go back to the partnerships. The more people that we have -- it doesn't matter who employs you, whether it's private sector or individual or government, it doesn't matter. If you've got a good brain and you want to jump into this, the ocean is wide open and we need people there. We need them collaborating across all these boundaries. It's not competitive. You know this is all about security of our way of life and so the more people we have doing that the better it is for all of us.

CHAIRMAN LA FLEUR: So you need a human to spot the patterns, but can the computer like toss up the data? I remember when we used to have the mainframe and you actually had the code. You're not going to actually be -- like I know you're too young to have had those punch cards that we had, but I mean you're actually looking for the

COMMISSIONER HONORABLE: Yes, I'll admit that.

CHAIRMAN LA FLEUR: But you know nobody has time to look at all the little things, but somehow you have to look at it electronically, right?

MR. SACHS: You could find a card in a fortran deck, yes.

CHAIRMAN LA FLEUR: If you got one wrong, it won't run.

MR. SACHS: It messes up the whole program. It won't work. And then you get to the end of the line and run

it again.

CHAIRMAN LA FLEUR: But there's the equivalent now, even though it's no longer a card where there's some thing in there.

MR. SACHS: Large datasets is the challenge because we're accumulating all this data, terabits of data. The human mind cannot begin to grasp this. This is the challenge that Google and Amazon and others have overcome where they look at very large amounts of data, use the power of computer to go find things and present it to a human in a way that our brains can interpret it. That's something we're also beginning to understand in security is how do bring something out so the human can see it and it's only through your eyes. We can't really taste cyberspace or hear cyberspace. We have to look at it because that's the way our brains work and so the challenge is how do you put something on a screen that a computer can express to an human so a human can understand it and begin starting to ask the questions and then the computer can go back and maybe answer those questions. A lot of work being done in the research community, a lot of work still to be done there, but data visualization is one of the big key items and security visualization is key piece as well.

CHAIRMAN LA FLEUR: It's fascinating. I know Michael is -- has stuff to say.

MR. ASSANTE: Thank you. I would suggest that in deconstructing some past incidents that have affected control systems particularly the signals would not be described as faint, but they would be described as deafening. In fact, some of the incidents would demonstrate that adversaries were experimenting. In fact, we've developed what we believe as models to look at in order to have a physical affect on a system it takes quite a bit of effort on the adversary's part in order to learn and know and have confidence that if they do something they're going to have a desired affect. And in the case of Ukraine, there certainly were observables and we wrote about those significantly with the EISAC about what to look for. And for example, some of the switches that uploaded most of (1:11:07.8) to they typically aren't touched by individuals. Once they're commissioned and tested, they're never managed. And when somebody goes out to touch them, it should be a big indicator that you know why are we doing that, right?

And also, I would say in the area you talked to earlier panels about data analytics and to Marcus's point, I've seen incredible prognostic technology advancement in this industry. In fact, arguably, I've seen individual utilities understand machines to a level of fidelity that is impress to be able to predict failure so they could take

failures on their own terms. I believe we have the technology to apply that for the cybersecurity challenge.

Again, if you go with the basis that, in fact, this new malware that we've discovered it just doesn't work all by itself. You have to get it into position and then you have to have this confidence that you understand exactly how the utility's operating breakers with the protocol, it's AD&P3. There's different ways to do it. And in order to experiment, you want to catch them in their experimentation. Prognostic technology could see the slightest tampering, an unauthorized circuit breaker operation in a small part of substation is something that can be detected. And I do believe that the industry has the capability of going down that road. They need the flexibility to try to conduct that innovation. I've been working with people like General Electric. GE has been looking at that. They understand their machines very well. They're looking at how can they use their models to identify tampering within those same systems. So I believe technology and that data analytic you talked about earlier is a tremendous opportunity for us in order to start outpacing the attackers.

CHAIRMAN LA FLEUR: Thank you. I was going to ask who could we learn from. We just heard Google, Amazon, and GE -- I mean people out there that are doing this.

I think it's related, but you talked about, at least in your written testimony, about Internet signatures, which I guess where you see where something is coming from and Commissioner Scott mentioned the fusion centers like in Topeka that compare one set of data to another set or data or whatever. Do we have the right protocols to share that? Do we need to do things differently so if one company sees something it gets to the EISAC and gets to other places? I mean I don't understand it well enough to know, but it seems like it would be rich area to prevent problems.

MR. SACHS: I'll give you a brief answer and then I'll pass it to the Commissioner, but oftentimes organizations like us or a private sector group or the government will see something and want to pass it to others. We use a process called TLP or Traffic Light Protocols to handle the sharing of information. So when you discover it, you have to be careful about it. You don't want to just broadcast it to world because your adversaries may see, but you wanted to give it to a trusted partner who can do something with it, so you'll call it TLP green or amber or whatever.

On the government side, oftentimes, it's detected in classified channels and so it's got a classification wrapper on it and we have to get that wrapper off, get it down to unclassified. There's a delay there.

When the machines want to talk to each other, they don't understand any of that. That's a human hindrance and they love just chitchatting back and forth, but it takes a human to connect two computers together and often the humans are bound by legal barriers, bound by information and trading barriers, bound by fear that the adversaries might get in the middle and watch the machines talk.

So there's a lot of good technical things we can do, but there's a lot we need to do in terms of the human understanding of why we need to rapidly share and barriers that are artificial, largely legal, cultural, that we need to take off the table.

I know we often have good stuff we could share with others. Others have good stuff that they can share with us, but many times it's the people that get in the way, not the technology. That's not stopping us. It's the process. The Commissioner may have the same sort of observations.

CHAIRMAN LA FLEUR: Bob, I know you talked about fusion centers in your testimony. I know what some of what they do is confidential, but I guess are there ways we can share this data better?

COMMISSIONER HONORABLE: I think it's a great question because I think with some of the fusion centers that is the challenge, that if you don't have a clearance

you really can't really participate.

COMMISSIONER SCOTT: Well, that is something, as you're aware, New England is exploring. We have a fair working relationship with the Kansas Intelligence Fusion Center. We're exploring that type of activity, but Commissioner Honorable is exactly right. Obviously, that only works to the extent that the utilities involved have the appropriate clearances for obvious reasons.

So it brings in a world of other issues like spillage and mitigation strategies, but I will say at least in New England, and I think Marcus mentioned DOE CRIPs, not all of them, but most of the utilities we're working with on that type of activity are also using CRIP, so it's not one or the other. They're finding extra value having gone out to Kansas and worked a little bit with them. It's an exclusive club, if you will

CHAIRMAN LA FLEUR: In your perfect world, anyone, I mean how many people within a utility would have a clearance. I mean I got to a lot of briefings with CEOs. I mean I was the CEO. I didn't do the computers, right? I mean I was never a CIO. You'd be insane to make me one, so I mean you'd brief these people who might have clearances and I mean so how -- if we had a perfect system where the right people had the clearances, how deep would it have to go.

COMMISSIONER SCOTT: There's multiple questions there. What level of clearance depends on how deep you're going to go also. Generally speaking, in my view, at least to get started obviously there needs to be CEO buy-in. The CIOs ideally would be involved and then you have the actual people doing the work, right? So that I would argue for two or more, I think, depending on what you're doing and why you need that. And I say buy-in is as if there's a mitigation strategy that's developed based on that type of data that costs some money, obviously. Now that has to be sold up the chain for obvious reasons and I'm a regulator at the moment, so certainly get that.

That requires the buy-in, so at least to start I think you need more and my guess if the utilities were to go down this path that once there's a faith in the system, if you will, that perhaps could get lessened. So I'm not suggesting that clearances are easy. In a post-normal world, if I were on the federal side I would be wondering too how many of these do we want to give out, et cetera. It's a challenge.

CHAIRMAN LA FLEUR: And I wasn't arguing that CEOs shouldn't have clearances. It's just they're not going to operationalize it into the machines, I assume, unless they're very unusual.

MR. WALES: Let me try to provide a little

context to this, both the value and the potential overestimation of value in providing security clearances. I think we've used security clearances that we provide to the private sector and DHS itself has cleared somewhere around 1500 to 2,000 private sector owners and operators throughout the country.

They provide two purposes. One, is they're helping us, so when we have classified information we can share it with them and they can provide context from how the industry would view this information. Are there things because of their unique expertise and understanding and the kind of activities that they oversee that they could read into this intelligence that government analysts won't be able to do.

Second, it helps to provide broader environmental understanding of the nature of the threat. It is not going to help with network defense immediately. That's why we spend a lot of time trying to figure out how to get the kind of information that's going to make a difference to network defenders down to a classification level that can be share because when we bring 20 people into a room and provide them with a classified briefing they can't just go back to their office and tell their network defender put in the following classified hash into your firewall. You know it doesn't work that way and so

clearances are an important part of what we do in terms of the information sharing. We think it helps make sure that we are on a common baseline with the leadership inside of organizations and with the key people who have to monitor their networks, but it is not going to be a panacea for even emerging threats and risks.

It's not going to stop necessarily the next Ukraine if we have indicates of the kind of activity or the kind infrastructure that that cyber operator was using to target those networks. So we think it's important, but it is, by far, not going to be enough.

CHAIRMAN LA FLEUR: So I'm going to translate back what you said. It's not just getting some people clearances. It's getting the data to a level that it can be operationalized. Okay.

MR. MITCHELL: If I could just add a little to that, we always are pushing for the information to become actionable. You know get it out to the industry. It doesn't have to be classified. It's just utilizing classified information to inform an actionable alert that would come out through the EISAC or some other form. And then we, as the industry, would utilize our trusted networks of saying trust us. We're getting this information. We need to act on it. We need to move on something and it is of highest of importance.

Unfortunately, and Commissioner Scott brought up the issue with Burlington. That was followed. Everything was done right by Burlington and then they went through the mud in the media. We lost trust in the system with that, but we are rebuilding that through these efforts and we encourage that trust rebuilding.

CHAIRMAN LA FLEUR: I want to ask one more question that's on a different cybersecurity topic. One thing you hear a tremendous about is the increased cybersecurity threat from all the distributed resources and the Internet of things. Frequently, that is said by people who might have other reasons to not like distributed resources, so it's hard, as always, to unscramble this.

I generally feel like if we're doing our job in this building, then if something comes in from a distributed resource and it gets up to the Bulk Electric System it shouldn't be able to go across and be a cascading outage because we've stopped it at that level. But I have all these experts here. How much of an issue is this, the fact that we're going to have a lot more distributed resources and is there something we should be doing about it because it's very (1:22:24.6)(in the land? You hear it as sort of a throw away line in speeches. And by the way this going to become much worse because of blah, blah, blah, blah. Interested in your thoughts.

MR. SACHS: Just briefly, it's not the distributed energy piece. That's electricity physics that we worry about. From a pure security perspective, it's introducing a new device that you don't know about. It has possibly a connection to the open Internet that we don't know about and there are billions of people on the Internet that we don't know about.

In an earlier world, it's all protected. These things that connect together and produce and deliver electricity are private. When you bring in an Internet of things or anything that's connected, it doesn't matter what it's doing, if it's connected you're now extending what we call the attack surface. That is the fundamental issue. It's not the physics of it. It's not the politics of it. It's the fact that you're connecting the public Internet, possibly at the bottom, which could then open a door to come up through the bottom of the network through distribution and perhaps do damage.

CHAIRMAN LA FLEUR: So in the olden days, which wasn't very long ago, the meter on my house only the electric company could read it. It had a lock. I never touched it. It was just all there. But now if I have my phone and I can turn things on and off, then a lot of data is somehow around; is that sort of what you're saying?

MR. SACHS: It's again not so much the data. If

the meter can be reached anonymously by somebody we don't know about on the Internet, there could be a problem. If the meter can only be touched to authenticate it; in other words, the electric power company is the only one that can read it and talk to it, we're fine. There's no issue there. It's that unauthenticated piece that's the problem.

CHAIRMAN LA FLEUR: So is this a problem for the Bob Scotts of the world or is there something FERC should do?

MR. SACHS: No.

CHAIRMAN LA FLEUR: So it's at the distribution level, but it somehow -- Michael's going to help us.

MR. ASSANTE: I was going to suggest two dimensions. What we really need to watch out is the concentration. And when I say by concentration, it is the access and we like to do this. In a market-driven economy, we achieve efficiency and often in the achieving of that efficiency we build architectures were we actually concentrate to be able to touch lots of these things.

In fact, I've been amazed sometimes about seeing distributed resources throughout the country that's actually in a maintenance sense monitored at a single location. Now the question in my mind in these architectures is when we do interact with these devices in a distributive fashion when we're interacting how many should be interacting with it at

any one time? Most business cases means we're going to deal with one, two, three, or four machines to tune or make a change or adjustment, but the architectures allow for touching all of them. And these are the types of things from an engineering perspective we need to take note and so it does extend into the distribution systems. It does extend into renewables, for example. But again, I believe it's about secure architectures. There's lots of benefits for doing it this way. We should absolutely be moving forward in that direction, but we need to bring that security requirement into the engineering design of those systems.

MR. WALES: Let me just give you two ways of thinking about this. On the one hand, the distributive resources within a particular utility if those are protected the same way that they've protected the rest of their operating systems, meaning that there's not Internet addressable systems. You can't get to them from the outside. You can only get to them from inside of the network, then they're as well protected or not as well protected as the rest of the operating systems that they have on their grid.

If, however, those are Internet addressable, which means anyone in the world can immediately find that and begin to look for weaknesses, the adversary has a lot of

time and they will eventually find weaknesses in those systems. And if, depending on how the configurations work, if they get in they can move elsewhere and do a lot of damage. But I would say that's a little bit distinct from, I think, some of what you're hearing, which is kind of the second issue, which is just the large number of Internet of things potentially provides an adversary a lot of toys to connect with and then use those an amplifying attack on other infrastructure, which what we saw with the DDOS attack using the Mirai botnet both net late last year where they just created a huge, loud service attack because they were able to get contact with all of these Internet addressable Internet of things devices -- you know little things in your house that you don't even think about, but they're connected to your Wi-Fi. They're Internet addressable and an adversary can eventually get contact with those.

So in terms of where FERC is and where I think NERC is the question is how do these standards cover widely dispersed devices on a utility's operating network? What are the requirements for security around those devices? And if they're just part of their regular operating system, they are just now sitting at your home as opposed to inside of a substation they can be well protected.

CHAIRMAN LA FLEUR: But technically, jurisdictionally we're doing the Bulk Power System, so if

they're on the distribution side of the meter, unless they're going to come in, jurisdictionally, at least, the states would make the rules.

MR. SACHS: Only if you're talking about a grid device or distribution device, but what Brandon's talking about is much, much bigger. Could it be FCC? Could it be Consumer Product Administration? I mean there's a whole lot of other animals here that have to be brought in. It's not just a NERC/FERC versus states to have a discussion.

MR. BALL: So the key component of that from a utility perspective is the architecture of that infrastructure. You have to have the ability to separate your corporate network that has access to the Internet from your operational network or SCADA network. And that is probably the key to maintaining cybersecurity on anything that can be or could be controlled from outside of the utilities.

CHAIRMAN LA FLEUR: You didn't necessarily make me feel this wasn't a problem, but at least you made me feel like you understand it very well and that's a very good start.

MR. GOVINDARASU: I think that IOT is the new thing that anyway that comes small on the consumer side, but coming back to the bulk process that will sell. The smart grid technologies, like whether you call it smart sensors

like PMUs, like communications technologies, distributor controllers, all kinds of things they do increase attack surface, because those are IP-enabled devices. They are connected somewhere. You have more access points.

The question is whether those access points are available to adversity or someone outside. How do you protect that? So assessing that attack surface and also minimizing that attack surface of risks. I think those are important. It is not to say, oh, we should not automate, then we are going backward. While we are automating things, we need to make sure that a security is in place. There's secure architecture isolation, what kind of access control has to be in place or authentication and so on. I think it has to be carefully planned. That is where the standards come into place. A weak systems are allowable to be accessed outside. Some other things should not be allowed, then it should be within the parameter and things like that. I think it has some flavor of those things. But as we talk about IOT and other things, one has to be very careful about defining those standards and what those qualities are.

CHAIRMAN LA FLEUR: Well, thank you for that clarification because some of those smart grids are very much on the Bulk Power System. We're talking PMUs on big transformers and things. Thank you.

MR. BARDEE: So I just have a couple of quick

questions, recognizing that we are getting near the end of our day.

Mr. Assante, in your written testimony and again in your oral remarks, you reference an effort by INL involving consequence-driven cyber-informed engineering and you said that it's a way to engineer out the worst cyber risks from our critical energy infrastructure. Could you talk a little bit more specifically about that?

MR. ASSANTE: Sure. And this goes back to, I think, a question of an earlier panel, this idea of fallbacks or analog, but really the bigger concept is taking the strength of industry, which are the deep expertise and trying to understand what type of consequences a cyber attack can enable within the power systems or assets in which the utility controls. By taking that additional prioritization, this idea that consequence first, let's look at what would be something would be more difficult to recover from. I mean that allows them to really identify and understand at a very deep level how do these systems work and how have they been engineered as we've deployed them and then reconsider some engineering choices and tradeoffs.

Ideas like simply removing a soft cyber control and actually having a dry contact might be a very cheap engineering solution that removes an entire risk of a

machine being damaged irreparably. So the idea is to get that level of depth. It forces utilities to break through assumptions, thinking that we're done this way and that way and we find that there's a lot of false assumptions when you actually go look how systems are put together and what is possible. But also, again, it builds on the engineering strength of utilities.

And the reason why I believe it's absolutely necessary is adversaries today are demonstrating the capability that we must, as defenders, go beyond cyber. I appreciate that some of folks here believe in separate is absolutely important in terms of separating your business systems from your control systems; however, the adversaries that we've watched are getting good. They understand that separation will be there. They're developing delivery techniques to beat that separation. Two factor VPMs have been defeated by certain actors around the world. So some of these controls that we rely upon are no longer as effective as we believe they are and so going beyond that to understand, I think, what is our strength in applying engineering to this problem has lots of benefit.

And again, when we talk about focusing on large outages and losing big parts of the system that's where a constant-driven approach really brings you very quickly. You begin to understand that it might an aggregation of how

we're interacting with several low or medium CIPs assets as defined by the standards because the way we've architected our interaction this is an area that we need to go back and readdress how we're engineering. It will inform cyber defense efforts too. Having a deep level of understanding goes back to your cyber defense strategies.

It allows you to identify jump points where adversaries need to get to in order to be able to affect some of these things. And I would also argue as my last point the malware that we've seen the way it attacked the system to cause disruptions is absolute a normal way should that the system should communicate. It's using the industrial protocol that we have implemented to open a circuit breaker.

There are some features within the malware, like an exploit against protective relay, which would have a signature that looks like it is something that is non-normal, but everything else looked absolutely normal. So I would encourage utilities get a deeper visibility into how systems communicate and that begins with an engineering understanding, which I know the utilities have and possess that capability.

So working with our partners, we believe that's going to provide the biggest reduction of risks because the type of risk we're most worried about come from your

significant risk-type of dimensions. It's not from the 12-year-old hacker or the 14-year-old hacker, if you will.

MR. BARDEE: So to me, it sounds a little bit like an idea I've heard about in the context of our physical security standard, CIP14, where utilities will look at their system and say, well, for now we're going to protect the ones that are critical, but in the future we're going to build out our system in a way where we don't have critical substations. We're going to reduce our risk by redesigning going forward.

MR. ASSANTE: That's absolutely right. The long-term learning as to what enables a terrible consequence through cyber means what could happened informs design decisions in the future and so we're starting to see some of that activity as we're engaging in some of these methods with industry and industry partners. So I believe that's absolutely right and bringing in the suppliers to partner on how they are architect to design their solutions is a vital aspect to this as well, so this really an opportunity for shared learning and the ability to be able to move that learning. And I believe a lot of what I've seen in deconstructing real-world events would indicate that that type of thinking is important.

I'll give you one last example in a nuclear context and I'm very proud to see the United Kingdom is

adopting this. We've moved to digital safety systems for our advanced light water reactors. That's a move away from analogs. You had to. But the question is not an analog device, but the question is should we be using general purpose controllers in technology for that safety system or should we have a fallback system that is a highly deterministic and very difficult or I would say limited programmable device that is performing that final safety function to avoid what could be a consequence that's not tolerable.

Those types of engineering efforts need to be understood by the suppliers. Economics will drive us one way, general purpose. Knowing where the limits are and where the thin line, if you will, would be for consequences that we cannot tolerate would require us potentially to go the other direction.

MR. BARDEE: And one last topic I wanted to raise with Mr. Sachs on the reporting requirements for cyber security the State Reliability Report notes that we had no reportable incidents 2016 and even in 2015 and I understood from the report itself, and I think your remarks or maybe Mr. Cauley's earlier in the day, that you all are taking another look at are there other metrics we should be looking at. Could you describe that a little bit?

MR. SACHS: Yes, thank you, Mike.

So this kind of goes a little bit to what Mike's talking about is what's the consequence you want to avoid and we want to avoid loss of load, so we go and look and see has there been any loss of load caused by cyber and the answer is no, or by other security events. And so you report that and say all is well, but it kind of gives a false impression.

Yes, the consequence has been avoided, but it doesn't mean there's not a problem or that there could be a problem or something hidden and that's our challenge, guys. How do we go look for those types of things we can see, measure, have reported to us, and begin to do that analysis that even though there's not been a lights out or loss of load or the consequences we don't want to happen that we still become cognizant of what else is going on and so we can get that early indication.

Currently, as you know, we've got mandatory reporting at certain thresholds and that's working fine. Then we have voluntary reporting beyond that, a lot of improvement we can do there, but also we have to recognize we have seen a lot of improvement in the last few years. The amount of voluntary reporting is definitely on the increase and we want more of it. But like anything else, there's that fine line of do you want to move out mandatory piece so people feel compelled to report, which means

they'll only report what they have to report or do you incentivize the voluntary side so people would feel more comfortable with voluntary sharing. They'd feel if I put something in I'll get something back out. We feel that's the proper way to go. What is that incentive? Don't know. That's part of what we need to work on this year and the coming years is what can we do to help increase that voluntary sharing.

Can we use the fact that the machines automatically record everything they see? You know the logging functions that are built into virtually everything. Can we get that because that's not an opinion? It's not a survey. It's facts that the machine is recording. Can we get those logs shared? Can we get telemetry off of CRIS and CAS and some of these other new programs? Can we study that telemetry and look for those faint signals that you hear us talking about?

These, I think, are areas rich for the next coming years of exploration, things we can do that don't require more mandatory sharing, but can look at what we're already sharing and see what we can pull out of that and then encourage more of that voluntary, particularly machine-to-machine type of sharing of knowledge.

MR. BARDEE: Then last question, again related to the reporting requirements. Whatever the reporting

requirement is or whether there's voluntary reporting or whether there's voluntary reporting on top of that that's much more rich right now the NERC Report puts out just a number and the last two years it's been zero, but in prior years there's at least been a couple of events, I think. Is it possible for the EISAC to take the information it has, whether it's mandatory or voluntary or it makes a difference which one, and provide at least some additional information about the nature of the event that have been reported. It would have to be at some fuzzy level of granularity and certainly anonymized, but ISC CER, for example, puts out an annual report that says, you know, in this sector we had "x" number of events last year. Is that something the EISAC could do?

MR. SACHS: I think absolutely that's something we can do. In fact, in this year's grid resiliency report the chapter on grid security is different from what we've done in the previous two years where we actually did look at 2016 what was reported to the EISAC and tried to tease out what can we learn about what was reported.

Granted, in 2016, we're still ramping up. In '17, we've already surpassed the entire year of '16. We've already accumulated in '17, which is good. So next year the report will be that much richer, but what you're hitting on is exactly the direction we need to go in. The EISAC pulls

in a lot of information. We analyze a lot of stuff; put a lot of reports out. We can also analyze what we've analyzed and create a much better picture, at least orally describing what we're seeing and what we're learning. What's going on beyond just what the machines are talking about, you're absolutely on the track that we're on.

MR. ADREJCAK: Just a couple of comments and then one general question, I guess. Greg, you'd mentioned earlier about phishing attempts. There was a report that came out today about a quarter of the Australian utilities were just hit with phishing attempts, so it's not something that's easily going away. I mean it's obviously still out there, so it's very on point.

Second thought, Marcus, you talked about getting these folks at a young age involved in cyber defenses. I was recently at a military exercise last week where we had all branches of the Military, along with a lot of friendly nations there, nice big scale drill exercise. They genuinely were excited about it, but what I found out was nobody wanted to be the defender. They all wanted to be the attacker and that seems to be the biggest problem I think we have right now is folks don't want to be the defender. It's more fun to be the attacker.

MR. ASSANTE: In fact, you know an assistant administrator is the defender. You talk to somebody who's

in 10th or 11th grade and you say do you want to be a cyber attacker or do you want to be a system administrator? You know what's the response? But much like in the Military, we teach young servicemen and women how to defend at the same time we teach them how to attack and you learn that your weapon, whatever your weapon system is, is both for defense and offense.

When we teach people how to be system administrators, we often shackle them and this is a big problem in the Military. You know thou shalt not do anything other than these things and if somebody bad comes in call this other group. You are not allowed to go elsewhere. So what do the kids want to do, they want to go work in that other group because they're the ones having fun because we shackle the defenders.

So that's part of this mindset we also have to think about and it goes to what many of us have been saying here. There's new rules we need to come up with, new approaches, new ways to thinking about not just for the kids, but even how we operate in this cybersecurity world that's very different from what we've been doing historically, which is more of a safety-oriented type of world and very predictable. This is not as predictable.

MR. ANDREJCAK: Mike, I guess my final comment is directly more or less towards Mike and I guess

Commissioner Scott you as well because you kind of tied this issue together, but I read a really great article that had both you and Robert Lee from Dragos in Wired Magazine that came out very recently, which really shows both yours and his dedication. This is not just a job, but it's obviously something we all live. This isn't like a 9:00 to 5:00 thing. When it happens don't call me at 8:00 o'clock at night. You guys dropped what you were doing to go address a big problem in the Ukraine and I guess I was concerned about what are your thoughts about getting the information out there quickly versus getting the information right, as Commissioner Scott had to deal with, with the Vermont issue?

MR. ASSANTE: It's a critical question, difficult. As you can imagine, when any events occurs there's a fog of war, if you will, as to what really did occur and getting the right people to take a look at that information.

First, I want to commend the Ukrainians for giving an unbelievable look to the United States Government as to what did occur and that's important. This idea of commitment to shared learning with folks is very important. I think by working in different capacities with FERC and NERC and the utilities industries and stuff, I think this is an industry committed to learning. I think there are massive improvements that we could do in deconstructing

incidents and being able to do that. That type of work needs to be done and it needs to be prioritized.

The tradeoff between quick there's ways to do this. There is what we say tippers out to the injury that says we're not completely sure about this, but these are potential indicators. Here's what you could do with it, but being careful as to say what you can do with it our should be doing with it is where I think we got in trouble a little bit some earlier events that occurred. And in the government holds the role of being -- and so does NERC -- of responsible risk indicator, meaning they are going to get to the real story at some level of very real detail and I think we worked through the stresses of that in terms of communicating about the first Ukraine event. It did take a long time and I think there were no immediate attacks that occurred, so maybe that was okay that it took that time, but in this space we won't have that luxury potentially in the future.

I really worry about a campaign of attacks and I think if we start to experience that we will be forced to very quickly learn as much as we can and get information out as we're going in order so that other utilities can defend themselves.

MS. POINTER: I just had a comment and then a question. The earlier discussion about -- I think, Mr.

Sachs, you mentioned about telling those 13- and 14-year-olds to go out there and do stuff, I'm having the opposite conversation with my 12-year-old. So hopefully, I can convince him to be the administrator or the defender that you're talking about, but right now we're having some pretty -- I won't say difficult, but several discussions about what to do and what he shouldn't do.

My question is actually to Mr. Assante. I think Mike raised the question about engineering and I think you'd mentioned loads and I guess while you're here just what are your thoughts about the reporting requirement for low-impact assets? I know Mike mentioned about -- well, I think actually the conversation was more so on the medium and hot, but you'd mentioned loads, I was just wanted to hear what your thoughts are about loads.

MR. ASSANTE: Thank you. I am concerned that -- and I think that the standards have evolved in a wonderful way in terms of bringing more systems into scope, looking at systems and impact reliability and that's been very important. Some of the things we're learning in terms of real-world incidents could indicate attackers might be trying to operate against multiple utilities or a single utility in scale, which means now that something that we'd look at individually as an assets, as a low asset, but taken in an aggregate of being able to open circuit breakers at

multiple locations you know the impact is as bad as if you would've been attacking larger substations, 500kv and larger.

And that's a concern. It's obviously more difficult. What we should do is to think about how to architect our system to be able to allow an adversary to achieve that scale. Some things would require them lots of time and it would be difficult to do. Other types of architectures and ways we interact with technology make it easier.

I think if we take a good, hard look at that we might be able to accommodate both, the idea of assets and resources that individually when misused could cause big problems on the system. This mounds or malware that we're talking about has the ability to operate circuit breakers if you could deliver into place were it could communicate to enough substations.

And again, this is not easy, but if you could do that the scale problem comes in and so the load requirements in the standards today, as you know, wrap basic protections, not necessarily the type of protections. We talked about using VPNs. Well, those apply to certain assets, not others and so I think it forces us to go back and look at how we're interacting with a larger deployment of technology.

MS. POINTER: Thank you. That's all I have.

CHAIRMAN LA FLEUR: I just wanted to first start by thanking all of the panelists for your very thoughtful comments. I think it's been an excellent day. I think some views were rich, a very rich discussion. And thank all of the organizations you represent all day long for keeping the lights on, small detail, that's what this is all about. So thank you for what you do.

I want to thank the people on FERC staff for all the work in setting this up, especially Mike for chairing it, Lode White for doing a lot of the work to organize it, Sarah and others, everyone who pulled it together.

And finally, I just want to thank my partner in crime here, Collette. When we sat in this room last month, I said I hope this won't be the last time we sit in this room together.

COMMISSIONER HONORABLE: And it wasn't.

CHAIRMAN LA FLEUR: And I equally hope that today, but I'm less sanguine that there'll be a lot of other times.

COMMISSIONER HONORABLE: Cheryl, I feel like the runaway bride. I don't know if I'm coming or going.

CHAIRMAN LA FLEUR: I think you brought so much to this discussion and to the Commission, particularly with your relentless focus on customers and also your constant reminders of what we need to do with our state colleagues.

You know one of my favorite songs in Wicked is like -- I've heard it said that people come into your life for a reason bringing something you must learn and I really believe that. And you've also done a wonderful job representing the Commission, whether it's in Brazil or in the singing in the FERC chorus or all the other places you, so thank you for that. I will really miss having you.

COMMISSIONER HONORABLE: Thank you so much.

CHAIRMAN LA FLEUR: Not here, up there.

COMMISSIONER HONORABLE: Thank you so much.

Let me say to Mike Bardee, who continues to lead so well, I was mentioning to someone on the elevator I really don't think our jobs are the most important. Yours are because you hold this place up and you have the institutional knowledge and experience -- when I say "you," all of you and your colleagues and you have been committed to this job. And Mike Bardee went away. He went on a detail very far away. He went to Europe. And when he left, I said the only way I'm going to support this is if you come back, so he has. So thank you.

And I want to thank all of you, and especially those of you who are sitting in the softer chairs. You get a gold star because you didn't get to say a darn thing, but yet, you're still paying attention. Because this work is so important and we know today that challenges are greater than

they have ever been. And I remember when I began as a state regulator 10 years ago hearing that from someone "This job is more challenging than it's every been." Well, it is also and in 10 years it will continue to be, but I know -- and after this long day of our work together, maybe the second longest day of the year, that we are well prepared to be able to continue to work on the challenges that lie ahead.

It doesn't mean we have it all figured out, but it means that we have number of men and women across many sectors, yes, including our colleges and universities, who are committed to helping us solve very challenging issues and that really gives me hope and heart about the work that we can do together.

And let me say, too, to our FERC staff here thank you for supporting this effort that we carry out, not only every year, but each and every day the ways in which you keep electric reliability front of mind for us and I want to thank my staff as well. And to our fearless leader, who has been our chairman, so Cheryl was our chairman when I started here at the Commission and I, in fact, met Cheryl as soon as she became a Commissioner at a NARUC meeting and there were like a million people all over the place, like touching her, is she real? Is that the new commissioner?

And so from the moment that we met, Cheryl,

you've been so gracious. And even when I transitioned here, I joked that Cheryl's advisors at the time were my advisors because they helped me stand up my team and even though we haven't agreed on every single thing, we have agreed on most and it's been an honor to work along side you, along with our other colleagues who've come and gone.

And it's been an honor to work with you at all of the capacities that you've held here as chairman, as commissioner, as interim chair and hopefully, as commissioner and I'll be riding off into the sunset for the next journey. But this has been the highest honor of my professional career and it's so much so because of the men and women I've done it with, so thank you so much.

MR. BARDEE: So that will end the day. I thank all the panelists for their help today and other times when we've called on them and look forward to continuing to working on this mission with you.

(Whereupon, the meeting concluded at 5:10 p.m.)

CERTIFICATE OF OFFICIAL REPORTER

This is to certify that the attached proceeding before the FEDERAL ENERGY REGULATORY COMMISSION in the Matter of:

Name of Proceeding: Reliability Technical Conference

Docket No.: AD17-8-000

Place: Washington, DC

Date: Thursday, June 22, 2017

were held as herein appears, and that this is the original transcript thereof for the file of the Federal Energy Regulatory Commission, and is a full correct transcription of the proceedings.

Gaynell Catherine

Official Reporter

Document Content(s)