UNITED STATES OF AMERICA

FEDERAL ENERGY REGULATORY COMMISSION

Smart Grid Interoperability Standards

Docket No. RM11-2-000

FERC/NARUC Collaborative on Smart Response

Technical Conference on NIST Standards

NARUC 122nd Annual Meeting

Omni Hotel at CNN Center
International D Ballroom
100 CNN Center
Atlanta, Georgia 30303

Sunday, November 14, 2010

FERC Commissioners in attendance:

JON WELLINGHOFF, Chairman
PHILIP D. MOELLER, Commissioner
MARC SPITZER, Commissioner
JOHN R. NORRIS, Commissioner
CHERYL A. LaFLEUR, Commissioner

A G E N D A

Welcoming remarks

Charles Gray, Executive Director, NARUC 5

Ray Palmer, Office of Energy Policy and Innovation, FERC 5

Dr. George Arnold, National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology 8

George Bjelovuk, Managing Director for Marketing, Research, and Program Development at American Electric Power and Secretary, SGIP Governing Board 15

Richard Schomberg, Vice President, Europe Innovation Sourcing & Transfer, Electricite de France and IEC Smart Grid Standards Chair 25

Daniel Thanos, Chief Cyber Security Architect, Gentlemen Energy and Cyber Security Working Group, National Institute of Standards and Technology 33

Discussion and Closing Remarks 37

P R O C E E D I N G S

(10:38 a.m.)

THE CHAIRMAN: This is a little unusual; what we're doing here now, we've shifted over to a technical conference of FERC, the Federal Energy Regulatory Commission, that is being done within the Smart Response collaborative, and I appreciate NARUC for allowing us to do this very much, and doing it in the venue.

And also, it's a little unusual that I'm starting. This is a staff-led technical conference; normally it would be led by our FERC staff, and this is going to be led, backed by our staff, by Ray Palmer, which I'll turn it over to you, Ray, in just a moment.

But I wanted to get on the record a number of things to ensure that we all have our expectations in line as to what we're doing here and why we're doing this.

This technical conference by FERC is for the purpose, to review information on Smart Grid Interoperability Standards in general. We have a number of panelists here, and Ray will introduce them. But I wanted, from a procedural standpoint, to lay this out for you; and procedurally, I think the best thing for me to do is to read some of our notice of this technical conference, and I'll do that.

The Energy Independence and Security Act of 2007

lays out the policy of the United States with regard to modernization of the nation's electricity transmission and distribution system and directs the development of a framework to achieve interoperability of smart grid devices and systems, including protocols and model standards for information management. EISA directs the National Institute of Standards and Technology, NIST, to coordinate the development of this framework. Once the Commission is satisfied that NIST's work has led to "sufficient consensus" on interoperability standards, EISA directs the Commission to "institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."

So that is our basic charge under the federal legislation.

At this point, and you'll hear more, as part of this technical conference, NIST has a group of five standards they've been working on, they have posted. The Commission, however, has not made the determination yet with respect to whether or not there has been sufficient consensus on these standards to initiate rulemaking. I want

to make that very clear.

And if we do that, then that would be the point that the Commission would initiate a rulemaking with the issuance of a proposed rule, it would go out for comment. Prior to that, it may be that we would want to have additional technical conferences on a number of issues, including the issue of whether or not there's been sufficient consensus in this first group.

So we do have a way to go here procedurally, and I do want to make clear what the procedure is. So with that, I wanted to get that on the record; with that, I'm going to turn this now over to Ray Palmer from FERC to be the moderator in charge of the technical conference.

Ray?

MR. PALMER: Thank you, Mr. Chairman, and good morning. Welcome to the technical conference.

At any rate, I'd first like, before we actually get into the speakers, I would like to ask Chuck Gray from NARUC to make some comments.

MR. GRAY: Thank you, Ray.

Good morning, everyone. Thank you all, and thank you for coming out on a Sunday morning. I'd like to welcome you all to NARUC as well as to this technical conference, and I'd like to thank the Chairman and Commissioner Centolella for their leadership by putting this conference

together.

I was thinking about this, this is an historic occasion. I can remember, it's been a long time since there's been a noticed joint conference between the state commissions and the Commission. Those of us who read the Federal Power Act for fun and pleasure would note that there are provisions in the Federal Power Act that give FERC the authority to hold joint conferences with the state commissions, and I think this is a fine example of implementing what I think is an often-neglected part of the statute, and it probably should be used more frequently.

So thank you for being here, and I look forward to a very productive session. Thank you.

MR. PALMER: Thank you, Chuck.

This technical conference has been noticed under FERC Docket No. RM11-2-000. I believe that this is being recorded and a transcript will be available to the public.

The technical conference is something, as the Chairman noted, is related to the Commission's responsibilities under the EISA 2007 legislation. I would just note that there is already a substantial record of smart grid policy and public input related to the policy statement that the Commission issued in July of 2009, which was preceded by a closed policy statement in large number 70-some comments, very thoughtful, good comments. And that

is all available on the FERC website under Docket No. PL09-4.

Procedurally today, we do have an excellent group of speakers. They've each been given a time allotment, and we've asked them to please stay within that time allotment. I believe we have a timekeeper to show them signs when they're approaching the end of their allotment. The plan is to have all the speakers go first, and in the end we will have questions. First because this is a FERC technical conference from the FERC Commissioners, and then from the State Commissioners who are at the table. In the unlikely event there's any time after that, there may be staff questions.

I should note also that the next session will follow up on the topics of federal-state coordination and cooperation. That session is being facilitated by Rich Sedano, and will again be for the benefit of the state commissioners to ask additional questions, and speakers will still be here, either following up or on other issues.

During that session, there will be some cards distributed that if there are questions from the public, the questions must be written on those cards; and if there is time after the state commissioners have asked all their questions, there may be some time to answer some of those questions.

So with that, let's move quickly to our first speaker, George Arnold from the National Institute of Standards and Technology, who has been leading the effort to review all the standards which led to the identification of standards that are the occasion for this technical conference.

Mr. Arnold.

DR. ARNOLD: Thank you very much, Ray. It's a pleasure for me to be here.

The first slide, please.

So I'd like to discuss the first group of standards that in NIST's judgment are ready for consideration by FERC and state regulators, and I'd like to cover three topics. One is the process that got us where we are today; I'd then like to discuss the specific, the five standards that we've identified; and then I'd like to close with a brief discussion of how regulators might think of these standards, and what it may need to adopt those standards.

Go to the next slide, please. This is a buildup, so I will ask you to click as I go through the points.

The process started in April of 2009. Phase One of our activity, which went through August of 2009, was conducted through a series of public workshops that involved hundreds of organizations and over 1500 participants to look

at the standards that would be needed in the future smart grid.

In April of 2009, as a result of the first workshop, we posted a list of 16 standards that were identified through that workshop, and invited comments through the Federal Register. Subsequent work, including work done under contract to NIST by EPRI was published, noticed in the Federal Register soliciting comments.

The result of all that work culminated in the issuance of a draft -- click, please -- in September of 2009 of a Release 1 framework. Comments were solicited through the Federal Register and published in final form in January of 2010. This document identified 25 smart grid standards and an additional 50 listed for further review. At that time, no cybersecurity analysis had been done on these standards.

I should mention, by the way, the five standards we're talking about today were among the 16 original standards identified back in April of 2009. So we've gone through a fairly long review process here.

In parallel to all this -- click, please -- NIST established a new public/private partnership called the Smart Grid Interoperability Panel, or SGIP, to continue the ongoing evolution to support this process. One of the aspects of this is the cybersecurity working group in August

of 2010, a NISTIR 7628 providing guidelines for smart grid cybersecurity was published; and one of the tasks of this working group going forward is the review of each of the standards being identified through the process; and their review of the first five standards shown here was completed in October of 2010.

Click, please -- so the last step of this process was a letter from NIST to FERC October 6th, 2010 identifying these initial five standards and providing a narrative containing information that would be useful to regulators in their consideration.

Next slide, please. So the five families of standards -- it's important to recognize that there are many documents underlying these standards -- are listed here, and don't be scared off by the numbers. There's a lot of technical detail. I'm going to try to make it very simple for you by explaining how you can think of the functionality that these standards provide.

Imagine, if you will, that we were conducting this meeting and each of us only spoke one language, but that amongst us we spoke many different languages; so some of us would speak in English, some of us French, some of us Spanish, some of us Russian. Imagine how difficult it would be for us to conduct business. Out of frustration, we might quickly decide we need an interpreter to help us, and that

would be expensive and very time-consuming. It would be difficult for us to work.

The first four standards on this list provide a common language so that we can all communicate in the same language; it provides a common dictionary and a common grammar that's useful for computers interacting with devices in the grid to communicate with one another.

Now imagine that this meeting, instead of being an open public forum, we're going to be discussing very confidential and sensitive information and we want to make sure that there were no eavesdroppers or people who could disrupt our proceedings. We would need security.

The fifth standard on this list addresses the security aspects that are needed to ensure that the communications can be done confidentially and securely.

Next slide, please.

So why is it beneficial to have such interoperability standards that provide this common language? Well, for one thing, it reduces cost; it allows utilities to obtain the best solution for different vendors and have them work together; it streamlines processes, it allows utilities to have different applications supporting different functionality in utility operation to exchange data in an accurate way. For example, asset tracking, work scheduling, outage management. These things can all work

together through the common data language.

Besides security standards, addressed as risk management by ensuring that these interactions are secure, and having these open standards avoids the historic problem that we've had in the utility industry of vendor lock-in with proprietary solutions.

So pictorially -- put up the next slide -- I'd like to illustrate where these standards apply in the grid. They're really at the core of the grid's operations. Click, please.

The first standard, IEC61970, provides this common language or common dictionary or data model and the grammar for communication that deals with operations primarily in the transmission domain. Describe the components of the power system, relationships between them in a structured way similar to how HTML is the foundation for a common language in the web.

Click, please. The second standard, IEC61968, provides the same type of functionality, but now in the distribution part of the grid.

Click, please. The next standard, IEC61850, deals with substations and provides the common language for describing the devices in a substation, how they can interact and a grammar, if you will, to allow control of these devices in a multi-vendor environment.

Click, please. The fourth standard, IEC6870-6, is an inter-control center standard that allows control centers within and among utilities to exchange critical real-time information such as time series data, event notifications and accounting data. This standard is used today in almost every utility.

Click, please. The final standard, IEC62351, addresses cybersecurity. It specifies means through which authentication, authorization access control, intrusion detection, encryption and this sort of functionality which is critical to secure operation is enabled.

Click, please. Now why do regulators care about these standards? As I mentioned, these provide benefits to both utilities and the customers by allowing the integration of new systems from different vendors to provide new functionality, to be integrated with much less effort, by having common standards for these sort of basic data elements, the possibility for vendor competition and avoiding vendor lock-in is there. This enables innovation to occur in the functionality as opposed to in the way that we describe things. This drives down cost, ensures uniformity throughout the grid, and as I mentioned, it does it in a secure way.

Now it's important to understand that the standards we're discussing today, indeed almost all of the

standards that you will consider over the course of time in the grid modernization are not static. They continue to be maintained and updated to reflect evolving technology and requirements, a normal part of the standards process.

I'd like to move on now to the question -- what does adopting these standards mean? Next slide.

There are at least three different ways in which standards get adopted in practice. Many standards we can consider as purely voluntary are already in widespread use in the market, and may not require any regulatory action or consideration at all. If you think of Wi-Fi or Ethernet, these are examples of standards that almost everyone would agree are in that category.

There's a second class of standards in which there may be a need for some encouragement to help accelerate their adoption in the market and displace proprietary solutions as we move forward. There are a number of ways regulators can encourage these standards without mandating them. For example, by allowing cost recovery of systems that have employed the standards.

And finally, there are standards that are so critical to safety, reliability and security that they may be need to be mandated. Last slide.

So as you consider these standards, it's important that each of them be reviewed to determine the

relevance to the jurisdiction in which you operate. What does it mean to my state, for example? Do they enable an existing or envisioned policy to be cost-effectively implemented? Will, could or should a standard impact previous, current or future proceedings or rulemakings? And then, what can I do as a state regulatory agency? You can analyze existing dockets for applicability of these standards, analyze the standards against core policy objectives, build guidelines for when and how utilities should consider them. Some you may choose to mandate because of their importance, or you may use them to support utility proposals based on these standards.

That concludes my remarks, and I'd be happy to entertain questions later in the conference.

MR. PALMER: Thank you very much, Dr. Arnold.

The next speaker is George Bjelovuk, who is appearing here as a representative of the Smart Grid Interoperability Panel and also as a representative of his utility, American Electric Power.

MR. BJELOVUK: Thank you, Ray. Commissioners, good morning. It's a great pleasure for me to be here today.

George introduced a lot of the NIST interoperability standards work that's been going on for the last year and a half or so, and I wanted to at least provide

you a context from the Governing Board and from the utilities' perspective on that work.

This slide gives you an example of the size of the Smart Grid Interoperability Panel, and it's daunting that in some levels we've got more than 1700 individuals involved in the dialogue and the discussions on the standards development representing 600, over 600 organizations from a wide variety of stakeholders, some 22 stakeholder categories that these folks live within.

NIST created the Smart Grid Interoperability Panel to really provide some structure and oversight to the development of standards, and really create an entity that would be able to continue on and move forward in the standards development effort going forward.

The organization is open to any entity, and there's no cost for membership; it requires participation, though; and that participation is measured by an organization's participation in the working groups and its willingness to vote on measures in the organization. Next slide, please.

I like to refer to this as the org chart for the SGIP. Some of these efforts are somewhat difficult to follow, and I'll just very quickly review this and talk a bit about a few things George mentioned.

When NIST brought the task from the EISA 2007 and

recognized they wanted to catch up to work that was already in flight, in many cases, and the architecture council had provided a great forum to create the first of a series of domain expert working groups. NIST engaged the Electric Power Research Institute to further facilitate some broad outreach workshops, and ultimately resulted in the creation of this structure for the SGIP.

There are coordinating functions, there's a business operating policy group, a communications marketing and education working group, and one that's a program management office; core steering committees and working groups are on cybersecurity, architecture committee, and the very important work of the testing, compliance and certification group.

NIST retained the services of a third party administrator, and you see the SGIP administrator across the top of that, and the Governing Board, NIST, and the SGIP officers really provide some governance to the whole structure.

I'll point out that as the work of the SGIP identifies standards gaps, or standards that might be modified or further refined. The commission priority action plans, a group of individuals whose singular mission is to look through that gap for a standards improvement opportunity and make a presentation or proposal to the

Governing Board. Next slide.

This gives you a first cut process -- a draft process, if you will, of how we think this process will occur going forward, and this is a proposed process, it's a work in progress and still a lot of refinement to do there.

I'll start with the long rectangle at the bottom; it really represents NIST's framework that George Arnold mentioned earlier, it was version 1.0, that framework, within which it describes standards, interoperability standards and a roadmap for how we might use those in the smart grid deployments around the country.

We envision creating a catalog of standards, going forward, and if you think about how the catalog of standards would be created, it's much like that roadmap was created in the first place. Standards development organizations really have a responsibility to maintain and develop standards for parts of our history, and NIST identified in that version 1 of that document 75 of those that are potentially ready for adoption, and that became part of the first framework.

As we identify those priority action plans and gaps in those standards, you'll see the priority action plans interacting with SGOs, ultimately resulting in a proposal to the Governing Board for a new standard that might be adopted. We envision a process following a

revision to the smart grid interoperability roadmap document that was created, and ultimately following the process we initiated with the first five of these standards, a letter from NIST to FERC on that topic.

Next slide, please.

So from American Electric Power's perspective, this is a quick slide of our service territory. We serve 5.2 million customers in 11 states; we interact with 11 state regulatory commissions in the room as well as FERC. We're an electric service provider in most of those states, and we operate that business through the operations of our seven operating units.

Next slide, please.

So a quick update on what we're doing with 'smart grid,' and I put it in quotes because I think smart grid is a term that is evolving as we speak, and we've heard several discussions of what smart grid means to the regulators in the room this morning. So next slide.

Back in 2008, working with the Public Utilities Commission in Indiana, we recognized an opportunity to collaborate. So when we talked this morning about shared risk, we had an opportunity to do a 10,000 meter pilot in South Bend, Indiana in conjunction with the Commission staff and the Consumers Council to really explore these opportunities. What does a smart metering system do? What

does a smart distribution network do? We had to deploy two tier, two season time of use rates for -- those folks put in some distribution automation capabilities, and field tested for the first time the use of programmable communicating thermostats as a demand response device.

That project has been in production since early in 2009; it's been under evaluation for just about a year, and we expect to make a formal presentation to the Commission staff in Indiana early next year when the results from that project come in. Next slide.

In Texas we operate as a transmission distribution service provider, a wires company if you will, in the ERCOT electricity market, and the legislature there passed an automated metering system, AMS rule that enabled TDSPs to present to their regulator in Texas a plan to do full deployments of smart metering systems in Texas.

Our project was approved, and we're in year one of a four year deployment that, it's about a million meters, a $384 million project was approved there by the Texas commission.

Next slide.

When the ARA occurred or was passed, introduced to our industry, we had two additional opportunities to expand our smart grid projects, the most famous if you will of those is the smart grid demonstration project that we

were doing in Columbus, Ohio. We were selected by the DOE as one of eight or ten smart grid demonstration sites, and that project really includes a wide swath of a fairly robust variety of technologies that we'll be distributing and evaluating over a 42-month DOE project, including 110,000 meters -- someone, Commissioner Centolella suggested this morning that we deployed at a scale big enough to really extract some value from; we believe we've got a statistically valid sample of our customer base, and should be able to derive some analyses from understanding how the technologies are deployed.

We're doing smart distribution systems in volt control and 70 distribution circuits. And expanding the work that we did in Ohio, by doing a two tier, two season critical peak pricing, a rate offering as well as a pilot of real-time pricing, where we'll use the five minute PJM clearing price as the signal into a technology platform that we'll deploy in a thousand customer zones to understand how real-time pricing might be adopted by consumers en masse.

Next slide.

And finally, we heard this morning the work going on in Oklahoma, we're very pleased to be part of that work. When the NARA funds were distributed to the states, the State of Oklahoma decided to create a revolving loan program to make available funds to do energy efficiency

improvements. We'll be working with the Oklahoma commission to do a 15,000 smart meter deployment, and really prove this concept of how providing energy usage information to consumers might actually have a conservation effect. And really the focus of that deployment is really to explore those areas and ultimately provide a report to the commission. Next slide.

I'd like to close with a few perspectives on the standards that NIST announced to FERC, and standards in general. AEP selected the IEC standards for its transmission operations, that we believe these standards have been well established in the industry for many years. The inter-control center communications protocol, or ICCB was called that before it was called 6870-6, and so we've been using that standard in the interaction of our control centers for many years.

We believe that the IEC standards really provide a framework for harmonization opportunities as those exist. So in places where, using George's vernacular, where we're speaking different languages, we believe some of these IEC standards really can become the language that we can all use to communicate more effectively with one another.

Next slide, please.

The nation's electric system is at limited interoperability until now except in the bulk system, bulk

power systems really had their interoperate really driven by the NERC reliability regions and the wholesale market design. Utility distribution systems are by their nature separate, and don't frankly need to interoperate with one another, and the investments that we make there are long-lasting investments. So when we're worried about vendor lock-in, we're frankly more worried about distribution asset lock-in. We make an investment and we expect those investments to last for many years. We don't want to have to go back and review those as frequently as some industries have done.

We think the smart grid deployment really prioritizes the interoperability of consumer interaction with the grid, and that's really where we need to prioritize most of our standards development. So if you think about common methods of communicating with consumers across 11 states, we'd like to not have to do that eleven different ways. And so if we can think about focusing on the interface between our customers and the electric system, that really frankly shapes the priority of what we need to do.

Last slide.

I'll end by saying that the smart grids are being deployed in advance of formalization of standards, and I think we need to recognize that cybersecurity is a critical

component of that. And so where we don't have standards, we need to make sure that the technologies that we're deploying are secure and that regulatory approvals that precede this NIST standards formation and some adoption plan that I suspect will get developed as FERC and NARUC work together, we'll need to make sure that we have those opportunities for recovering models that we got in place to continue, even after that work.

Standards will need to coexist as they are developed so we won't have a one-size-fits-all, a standard that we develop today will have to coexist with a standard that we develop tomorrow. We're not going to have the ability to upgrade our systems from one standard to the next over and over, what to think about this coexistence and cooperation between these.

And flexibility I think becomes critical. If we too quickly pick a standard and drive its requirement, we fear that the we might stifle innovation and creativity by the folks who manufacture and innovate equipment in this space.

Thank you very much for the opportunity to address the panel.

MR. PALMER: Thank you, George.

Our next speaker is Richard Schomberg, and Mr. Schomberg is the employee of the French utility EDF,

stationed here in the United States; but he is also playing an important role within the IEC, and has in many ways been leading within the community the smart grid efforts at the international organization level. The International Electrotechnical Commission -- full name -- is in Europe in terms of the headquarters, but the United States and about 30 other countries are members.

It does turn out that for these particular standards that have been identified by NIST, quite a bit of the initial work that led to these standards being adopted by the IEC was actually done here in the United States, by the Electric Power Research Institute and other organizations here.

So I'm sure that Richard will also talk about the ongoing relationship with NIST and the American interest, as standards are developed internationally.

MR. SCHOMBERG: Thank you, Ray, for the introduction. Thank you very much for having me today for this topic that I'm devoting a lot of time and passion to now for many years.

For full disclosure, I am also a U.S. DOE - Architecture Council member, and also in fact I am really not stationed anywhere; I'm just coming from the G20 in Korea, and I'll be, at 2 p.m. tomorrow, in Paris making a presentation. So actually --

(Laughter)

-- no, it's interesting because now those activities are no more located in the specific country. It's really international activities. And the IEC actually is headquartered in Geneva, but Geneva is everywhere and nowhere, right?

(Laughter)

That's the beauty of Geneva, which means that actually it's not a European organization. IEC is a virtual organization composed of national communities around the world; actually 162 countries are participating.

Having said that, there's also a -- a word on my background before I started. I had been designing very large complex systems; that's where I'm drawing my experience, and I have been also leading a team of forensic examination of very large projects that have been failing.

Having said that, I see the first slide is up already.

IEC is really one of the three international standards development organizations which is recognized by the World Trade Organization of the United Nations to actually help in removing the technical barriers to trade. And IEC is providing the global platform for 10,000 experts from under the CC2 countries for developing standards globally relevant for everything electric or electronics; as

IEC is developing standards, has been developing standards since 1906 on electric sockets, on car -- everything electrical in cars, or everything in power plants or control for nuclear power plants, or everything about the grid; or it can be wind, you name it.

So it's really an international standard body whose core business is the electric sector. Next, please.

So of course IEC is developing some technical standards, but which is not as well known, also developing standards about performance and about quality of service. And important to note, there is an official working liaison that has been voted and put in place between NIST and the IEC as outreach. That's very important, because we don't have that kind of arrangement with any organizations. And while IEC is collaborating closely with a lot of professional organizations of the electric sector -- that was somehow missed at the bottom of the slide, so I'm not going to spend time on this. Next, please.

So what is important to keep in mind is that the development of IEC standards is always done on a voluntary basis, from experts that had been assigned by their national committee to represent the interests of their country, and within each country it's really the responsibility of the national committee to actually make sure that they get the right cross-representation from industry and regulators and

government to make sure that they want the right representative to be at the table.

And it's very simple; each national committee has a vote to approve, modify or reject a standard. Of course the national committees can propose new work, the development of new standards. And what is very important is the last sentence of the slide. And there are a lot of subtleties in this; which is that the value of the standard -- see, the standards are not standard. Please keep that in mind; the standards are not standard, in many different respects. Which means that here, when we discuss about standards that may, some might think that it takes too much time to develop, actually it's because the value of the standard is the consensus which is built in. You want to be able to regenerate the consensus and trace how the consensus has been built. And this is really why those standards have the specific value.

Next, please.

So now about the five core family of standards that are being recommended by NIST. They were developed in one technical committee that has officially registered 28 countries and 16 other countries are observers in this work. They are absolutely essential within the smart grid, because as has been explained by Dr. Arnold, definitely if you have a new smart grid project requiring to develop those adapters

and gateway translate the language, then it costs a lot. But actually this is not the worst.

The worst is that very often those adapters become some kind of bottleneck, and even worse. What I see in many, many projects in my forensic activity is that they just become over time some kind of land mine. And I pause here so that we keep that in mind.

So using those standards allows them to be, to avoid this and say it's a very powerful insurance, and of course it allows us to become vendor-neutral. Those standards have been, are universally recognized. They are referenced in many road maps, of course, in the IEC. In this roadmap, I was in visiting China a few weeks ago, and definitely those are core standards of state grid of China.

So I was just in Korea two days ago, and they just raised their test ban, concurrently with the G20 summit. And trusting enough; they are explaining how they've been building this from scratch, within seven months, and which IEC standards they are using. I was very surprised that even in their PR center, they were actually highlighting the IEC standards.

And of course they are, they appear in the roadmaps of the European Union and also in Germany they've been investing a lot in this. But of course we have the excellent example given by AEP. We'd like to mention also

efforts -- I know from LIPA for many years on this. And I want to give three examples from EDF, my company.

So the first one is that there are 42 transmission system operators in Europe, 42. 42 transmission system operators for 34 European countries. And actually, they are all meeting within the ANSI organization, and they have made the decision to transition to use those core standards for transmission, the transmission part. And this is very interesting because -- well, I know well about this example, because EDF R&D has been appointed to transition the systems of those different TSOs, and the interpreter of the test.

Another example is that we are using a lot of equipment in our substations, and we have and do have a lot of substations; like something -- well, a cap of 100,000, let's say. And of course we procure a huge number of equipment each time, but it's in the genes of the company, where we always procure from many different vendors. And we have been testing equipment from five manufacturers during five years according to the 61850 standard, and this has proven excellent to actually fulfill our policy.

So I can see that I am growing short of time, so -- next, please.

So we have to keep in mind that those standards are actually continuously updated, because there is a

process within IEC to systematically review the standards every certain amount of time, which is typically three years. And it is very important, because actually the very challenge our smart grid is that the smart grid is going to evolve all the time; it's a never-ending evolution. There will be parts that will have to be retired and parts to be added, so it's very important to have very strong standards, and actually the five standards that EISA selected are technology-dependent, they are among the most mature; because we started development in 1988. They both evolved because we have described the large view before doing something; and Commission Binz gave interesting feedback from thinking in California. I mean here we'd be thinking a lot about the entire structure of those standards before developing just pieces of this.

So that means that when we come to develop those standards, we know which direction they're going to go. And they allow integrating, actually, new technologies and innovation, and that's very important. Because the standards, actually, it's sometimes a conundrum. But actually the standards are here to create freedom. If they are good standards, they really create freedom, because they can really create spaces where the vendors can compete, and this is necessary. We could not actually be having standards that the would tell everything in great detail,

and that would not evolve with a failure to be able to tap on innovation.

And now the last slide, please.

Future work is very simple. See, I don't know if you ever tried to read the standards, sit at your table and try to read one standard. Now we are talking about using 100 standards. And now we are talking about creating a lot of green jobs, where you're going to have a lot of young workforce coming in; how do you want those people being able to even use the standards?

So you can have strong standards, you can have conformity assessment in place -- well, the weakest link will be the people in the field who have to -- you just missed them. So this is a major challenge that we have undertaken within the IEC, to actually make usable, as much as possible, the standards, the internal complexity of standards development to the users. And we are developing a lot of systems to specifically guide and help the practitioners in the field; make the most of the existing standards while helping, managing actually the evolution of both of portfolio standards, and of course there is still a lot of work to come from the IEC. Thank you very much for your attention.

(Applause)

MR. PALMER: Thank you, Richard.

The next speaker is Daniel Thanos from General Electric Company, a cybersecurity expert with that company that was also a participant in the cybersecurity working group that was set up by NIST, and he is going to talk about the very important issue of cybersecurity and the work done in the cybersecurity working group.

MR. THANOS: Thank you. First slide. I'm sure everyone has PowerPoint fatigue by now, and we probably won't get to -- some more interesting aspects of this.

So as all of my colleagues here have said, obviously -- not just from the aspect of interoperability and having vendor neutrality and greater market freedom, interoperability - good and having open standards - good, but actually it's a key security driver. You really can't begin to do advanced forms of security, especially the ones that need to evolve that use much more advanced analytics and intrusion detection security for management and detection until you have a common data format and a common way to kind of peer into these critical processes and configurations that are happening in the smart grid. So from that perspective, adoption of these standards is very important.

Also, when you're creating an environment where you're moving away from what have classically been more proprietary systems and you're going to more open-oriented

systems, it actually enables more people to begin to look the internals of how systems work; and from a security perspective, that's critically important, because the more eyes and more understanding you have around things, the easier it is to find vulnerabilities, and to find ways to improve things that make those better.

So let's talk about a little bit of the review process we engage in at CSWG. As was previously noted, standards that are being identified are kind of being sent to a subgroup called standard subgroup within the CSWG that goes through an open review process. We have a standard template and a methodology to kind of go through the standards, review them, see how they map against the NIST guidance that was put out; that's from everything from high level security requirements down to cryptographic requirements, see how exactly they line up, and if there's any points where there needs to be some improvement.

Definitely, just focusing on 62351, it's a good initial evolution for the industry. There are some things that might require some revision. In the security community, we are even guilty sometimes of abusing terminology. Sometimes it's very easy to get terminology wrong or to use certain terms in far too many ways. And so there are some formational aspects that need to be revised. And of course because the NIST was just recently published,

we have to kind of hold back and begin to work with various standards and their cryptographic aspects and kind of align with that.

And of course this is nothing that's controversial; and all parties involved understand this, and are working to do this. And as a side note, within the IEC organization that I believe in and participate in actively, we are establishing a key management group for the suite of protocols to continue all the key management of the crypto that's going to be needed in the future.

If I could offer just some points as, you know, we've been able to give options. What we found initially is CSWG is very good, I encourage holding another commenting period, which I understand will happen, but I think it's really important to be very active in engaging the broader elements of the security community. Sometimes things that are -- have just come out of the one focused industry, can have issues. If you don't have other, broader experts looking at it, it's time to get a different approach, different way of thinking, so I think that's going to be really important.

And the last point is very important; in modern standards these days, it's quite an interesting map that's built in terms of standards that reference other standards, both within the body and outside of the body. So sometimes

even when you're writing something, it's hard to keep track of the standards that you're ultimately referencing.

So in the case of this standard, for example, there are newer forms of TLS, and other security protocols. There has to be some way to kind of account for using the latest and best in terms of those standards that you reference, so. Just important points there. Next slide, please.

I'd finally like to close, just putting on my GE hat for a second, I just want to talk about how we have been using the NIST work that was recently put out. I work in forming the technical roadmap for the company; certainly the requirements that we have in there are actually going into informing everything that we're doing, our product requirements or doing our systems development. It's being used as framework in multiple projects that I'm involved in; it's informed in cybersecurity training and education; I work with universities, I regularly work with R&D programs in universities as well, and we're kind of going through that and kind of using it as a roadmap for future directions in critical search and other areas of security research. The optimized and directing form.

One next step that I recommend, and we're taking action within CSWG to do is, we're going to be forming a design principles group to kind of take the -- you know,

write a better how-to guide, to make it more actionable for good product vendors or for utilities, for people involved in procuring systems and what not; and we're just working through a process to see where that work can be published. And that's all.

(Applause)

MR. PALMER: Thank you very much, Daniel. I want to first, I neglected to mention in the opening comments that this session has also been noticed by several states so that there are a records being created within certain state proceedings as well as the FERC proceeding.

Also, that we did get started a little late, and I was informed we would go until 11:40, about another nine minutes. We'll start with questions from the FERC Commissioners, starting with Chairman Wellinghoff.

CHAIRMAN WELLINGHOFF: I don't have any questions, Ray. Thank you.

MR. PALMER: Commissioner Moeller?

COMMISSIONER MOELLER: No thanks, Ray.

MR. PALMER: Commissioner Spitzer?

COMMISSIONER SPITZER: No, thank you.

MR. PALMER: Commissioner Norris?

COMMISSIONER NORRIS: No; I'll pass.

MR. PALMER: Commissioner LaFleur.

COMMISSIONER LaFLEUR: I guess we'll give our

nine minutes to all the other commissioners.

(Laughter)

MR. PALMER: Okay. So then we move to the state commissioners. Feel free to put your tent card up, or to raise your hand.

Commissioner Centolella. From Ohio.

COMMISSIONER CENTOLELLA: Thank you, Ray. And first of all, let me express my appreciation to FERC for allowing us to join in this technical conference. I do appreciate that, and I think this is an example of where we can take parallel action in a way that is very constructive, and we have noticed this technical conference in one of our proceedings in Ohio.

I guess my question to the panel is: When I think about these standards, there are certainly -- could be some, perhaps the cybersecurity standard, that in some instances we might, after hearing from additional parties, we might decide that that should be mandated in certain circumstances.

There are other standards which may have great value; for example, the common information model standards. I go back eight or nine years in my career before I was on the Commission, and was working with a large utility that did a series of communications and meter upgrades, but also very importantly moved to SIM architecture for its real-time

systems, with a resulting savings of some hundreds of millions of dollars.

So I think of that as something to be encouraged, and I guess my question is to -- how should state commissions think about accelerating the use of this standard, encouraging its use, and if we look at these five standards, how do they fit within Georgia's framework of mandatory recommended or encouraged, and voluntary, in your view, as we were looking at them in terms of the investments that we review at the state level.

DR. ARNOLD: Let me start, and my colleagues may have other views.

In terms of where they've given us some categorization of voluntary, encourage or mandatory; I would say cybersecurity is certainly something you want to consider, as the mandatory realm, perhaps; you know, always the unintended consequences when we do something like that.

But what's more clear to me is that the other standards are probably not in that category, for the following reason: There are legacy systems that prevail in substation automation, there's a protocol called DNT, which has been the standard, and it has a large footprint. It's not as flexible as the IEC standards, but there's no way we can rip it out.

So what we are doing is providing the capability

through mappings that a lot of these standards do coexist, and interoperate to some degree. That has to be supported.

Even in terms of the information model, the rural utilities have for a long time used a standard called Multispeak, which is more likely and more suits their needs, and that will continue to be supported in the future.

So we're addressing this through mappings between them; we've not yet considered these other two standards in our process, because they haven't gone through a cybersecurity review. But I think we want to encourage the IEC standards, but I don't think mandating them would be the right action.

In terms of the other category of purely voluntary, because it's already in live use, the inter control center protocol might be in that category; that's for the commissions to decide. If everybody uses it, there really is no alternative. So that's my thought.

MR. PALMER: Comments?

MR. THANOS: I have another comment. In terms of the cybersecurity, the IEC specific standard for the cybersecurity, if you're considering making something like that mandatory, I would look at, you know, very closely look at making sure it's appropriately revised and that it's road-mapped. Because there are some technical elements, and a lot of these working systems need to get worked out.

So it's not a magic 'on' switch. You'd have to road map it and have to revise.

MR. BJELOVUK: Ray, I'll just add one comment to both of those observations, and I'll reiterate a comment, tried to make it the end of my presentation before I ran out of time.

I think it will be important for us recognize that we need to have a coexistence of standards as we move forward, and even today in the workstation security department, when you secure your Wi-Fi network at home and go through that little configuration tool, there's five or six or seven options for how to secure your wireless network at home.

And I think we need to focus on requirements. What are the requirements of the industry in the adoption of standards? What are the requirements of our security model so that we define and adopt standards? I think if we focus on requirements and focus on driving our ecosystem of vendors to comply with those requirements in standard ways that these standards apply, I think we'll be able to drive convergence among the market players.

MR. SCHOMBERG: And a quick comment about that, return of experience. In the nuclear sector, the US NRC is referencing an IEC standard, actually, for the nuclear safety of instrumentation and control systems. So it might

be of interest to ask them, how have they been doing and what happens? If they are happy or was there return of experience? And actually, other regulators throughout the world are doing the same.

MR. PALMER: Chairman Binz.

CHAIRMAN BINZ: Thank you. Sorry for dropping the microphone right in the middle of your presentation. We may have a smart grid, but we'll still have occasional student commissioners.

(Laughter)

I want to thank the FERC for joining us here at this meeting and for holding a technical conference, and I also want to thank Dr. Arnold for his participation in Colorado. We've had an ongoing docket, investigatory docket on the smart grid. One of the issues we addressed was of how to approach the NIST-FERC standards; we will be adopting those as COLLR standards (ph) as approved by the FERC; and we are linking this proceeding up to our state commissioner proceeding.

I don't have a question, but we're out of time anyway. Thank you very much for being here today.

MR. PALMER: There was a commissioner -- did you have a question?

COMMISSIONER: Yes, thank you.

I guess this is such a monumental part of this

task, is getting the standards worked out; and as one of the presenters pointed out, that the standards will be developed as the investments are being deployed. So you've got a situation where this is evolving in front of us.

The thought that crossed my mind is, "To what degree will, as standards are developed and solidified, what about the notion of backward compatibility?" How backward compatible would the further generation systems be for what is being deployed today? I think about a 2G phone that can work on a 3G network.

Can anyone comment on that?

DR. ARNOLD: That's been very much front and center in this process; understanding how to evolve and also how to capture the value in already-deployed systems that we're going to continue to support in the future. So many of the what we call 'priority action plans' in the SGIP process are looking at interoperability between legacy systems and these newer standards that are, sort of the direction that we want to move in the future.

MR. PALMER: Okay. Thank you all very much. We appreciate the speakers doing their presentations and informing us, and we will be moving now into a session that is not a part of the official record that will go into the FERC docket and the other state dockets, I believe.

(Conclusion of Panel discussion at 11:40 a.m.)