BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - X

In the matter of :

SUPPLY CHAIN RISK MANAGEMENT : RM15-14-000

- - - - - - - - - - - - - - - - - -X

Commission Meeting Room

Federal Energy Regulatory Commission

888 First Street, Northeast

Washington, D.C. 20426

Thursday, January 28, 2016

The technical conference in the above-entitled matter was convened at 11:00 a.m., pursuant to Commission notice and held before:

COMMISSIONER CHERYL LaFLEUR

COMMISSIONER COLETTE HONORABLE

COMMISSIONER TONY CLARK

FERC STAFF:

DANIEL PHILLIPS

RHONDA DUNFEE

DAVID DeFALAISE

MICHAEL BARDEE

ROGER MORIE

JONATHAN FIRST

KEVIN RYAN

PATRICIA EKE

PRESENTERS:

PANEL 1:

NADYA BARTOL, UTC

JON BOYENS, NIST

JOHN GALLOWAY, ISO NE

JOHN GOODE, MISO

BARRY LAWSON, NRECA

HELEN NALLEY, SOUTHERN CO.

JACOB OLCOTT, BITSIGHT

MARCUS SACHS, NERC

PRESENTERS:

PANEL 2:

MICHAEL KUBERSKI, PHI

JONATHAN APPELBAUM, UIC

NICK WEBER, WECC

ART CONKLIN, U OF H

EDNA CONWAY, PEPCO

BRYAN OWEN, OSISOFT

ALBERTO RUOCCO, AEP

DOUG THOMAS, IESO

PANEL 3:

DOUGLAS BAUDER, SOCAL EDISON

ANDREW BOCHMAN, DOE

DAVID WHITEHEAD, SEL

ANDREW GINTER, WATERFALL

STEVE GRIFFITH, NEMA

MARIA JENKS, KCP&L

ROBERT McCLANAHAN, AECC

THOMAS O'BRIEN, PJM

Court Reporter: Alexandria Kaan, Ace-Federal Reporters

P R O C E E D I N G S

(11:02 a.m.)

MR. BARDEE: Good morning everyone. Welcome to our technical conference today. I'm Mike Bardee, I'm the director of the Office of Electric Reliability and I'll be moderating the conference today. I'd like to thank all of you for coming today, especially given the weather the city's been through the past few days. And also apologize to you for the delay in getting the conference started today, but some things we just weren't able to control and that was one of them.

Let me turn very briefly to the subject matter before I turn it over to others here. As I think all of you know, we issued a proposed rulemaking in July of last year. And in that proposal we proposed to direct NERC to develop a reliability standard to address supply chain risk management. And we asked questions about what should be the features of that kind of a standard and what requirements should be in it, and also about what kind of a timeframe should it take to develop that kind of a standard.

So with that as a background, let me just go over a little bit of a housekeeping for today. First of all, I would remind all of the speakers, including the people at the horseshoe here, that this is a public meeting

and it's being webcast as I understand and transcribed. So I would just ask everyone to be mindful of your remarks given the subject matter we're talking about, what you say will be public. Then turning to the schedule for today, given the late start we're going to have to modify the procedures a little bit. So I talked to staff and we've decided that we're going to limit each question and each answer to just 140 characters to keep it short. When we get to 140 just stop.

(Laughter)

Actually, the schedule is going to be like this: After I finish my remarks and some other opening remarks we'll turn to one of our staff members, Mr. Slobodnik, who will do a brief presentation about cyber standards or guidance by other agencies, then we'll bring up our first panel which will end around 12:45. We'll take a lunch break for about an hour and return at 1:45. And then the other two panels will last about 90 minutes each with a 15-minute break. And if we stay on that schedule we will be done at about 5 o'clock today, which is a little bit later than what we had planned, but would still allow a good amount of time for the opening remarks for each speaker but also for some discussion and questions afterward.

With that, I would turn to our Commissioners and

see if they have any opening remarks, starting with Commissioner LaFleur, please.

COMMISSIONER LaFLEUR: Thank you very much, Mike. And I'd also like to thank everyone for coming, our government colleagues and all the industry colleagues in spite of the weather. This is the subject I'm very interested in because I know I have a lot to learn, and I think all of us have a lot to learn on this subject matter. Because of the enforced snow days, I think I have heard more of the testimony than any other tech conference I've ever attended. But what I'm most interested in getting out of today is assessing if the standard is needed and how exactly a standard would add value and if there's other approaches to consider, which there were lots of words in the testimony about do a guideline and adopt this, and what those other approaches would actually mean, how they would be carried out, what specifically the Commission would do. So as always, as specific as the panelists can be, the more helpful it is about what you actually think what we should do and what it means to you. Thank you, and I'll pass this on.

COMMISSIONER HONORABLE: Thank you to Commissioner LaFleur and to staff and everyone in attendance. You all get a gold star; look at this room. And it's about supply chain management, who would have

thought? I want to thank you all because I think your mere appearance speaks to your interest in this. So I'm grateful that you made a track from near and far and that you weathered the sidewalks and roadways, and I hope you make it back safely as well.

So with the help of our distinguished staff, we've managed to assemble a formidable group of experts to educate us on this topic, including transmission owners, RTOs, trade associations, consultants, and technology providers. And I believe you are indeed the experts. So I, too, look forward to be educated. I will pop in and out today because of appointments and rescheduling due to the weather, but know that we are paying great attention to not only the topic but your particularity as well. I did want to thank you for your involvement, the comments that you've raised. For those of you that have proposed -- a technical conference on this topic, thank you in particular. I think we might all learn a thing or two today.

I believe certainly the panelists we will hear from today are responsible for the bulk power system from California to Maine to even my home state of Arkansas. So you come with a unique perspective and expertise that I think will enable us to tackle the challenges. And I'm hopeful that the challenges, that we will be able to see as opportunities, will include exploring current efforts of

managing supply chain risks and government and other sectors, and evaluating the need and whether there is a need, for new or modified reliability standards, and determining the proper scope of that. So many of you have passionate opinions on all sides; I look forward to hearing them. And most of all I look forward to our collective effort in securing our national infrastructure. Thank you.

COMMISSIONER CLARK: When I walked in I thought you all had been stranded here since Friday. If so, I apologize. Hopefully the accommodations have been good. There obviously is a lot of interest in this. When we voted this order out I think all of us knew be were exploring new areas of Commission authority and that there would be a lot invested in what we're doing. I appreciate the fact that you're all here in providing this input; it's a very important area. What I'll be looking for today is to add to the record and my thought-making process, number one, what the Commission is proposing, is it adding value to our reliability effort? And is it doing it in a way that's both meaningful and is cost effective and is effective in what it's trying to get at, or is it somehow missing the mark? And if it is missing the mark, tell us why. It's not easy to do so, but I would say the easier part of this problem is always identifying the problems and the challenges and the scenarios that might cause risk to

reliability. Always the more difficult part is what are the exact solutions and how do we implement that in a way that is going to be affective? That's where the lens I'll be looking at as we fill up the record.

Again, thanks for being here. Like everyone, I have appointments I have to juggle today, I will be in and out. But I do appreciate you all at this point.

MR. BARDEE: Thank you all. And with that, I would now turn to Simon Slobodnik, who is a member of the Staff of the Office of Electric Reliability who will do a presentation on supply chain risk management efforts standards or guidance by certain other federal agencies.

MR. SLOBODNIK: Good morning. My name is Simon Slobodnik. I will be presenting on the programs of several other federal agencies. On July 16th, 2015, the Commission issued a notice of proposed rulemaking for the reliability standards. In this NOPR the Commission proposed to direct NERC to develop new or modify reliability standards to provide security controls for supply chain management for industrial control systems, hardware, software, and computing and networking services associated with the bulk electric system operations. These security controls would help manage the bulk electric system supply chain. Other federal agencies have also proposed or issued guidance or regulations regarding supply chain risk management. This

presentation will describe the supply chain risk management programs.

In addition to producing the present budget, the Office of Management and Budget issued instructions or information in the form of guidance documents. These guidance documents apply to all agencies of the executive branch of the federal government, the agencies of the National Security Systems as defined in U.S. Code Section 3542. OMB recently released for comment several instructions that are in effect of the supply chain risk management. It is a draft guidance titled "Improvements of the Securities Section and Position".

On July 30th, 2015, OMB issued a request for comment on those draft guidances. The comments period ended on September 10th, 2015. OMB stated the increase in threats facing federal information systems demands that certain issues regarding information must be clearly effectively and consistently addressed in federal contracts. OMB's proposed guidance complies to information of any applicable federal agency regardless whether the information is hosted under federal information system or the internal information system of a contract. Slide.

OMB addresses five general aspects of managing supply chain risk: Security controls, cyber incident reporting, security assessments, continuous monitoring, and

business due diligence. OMB draft guidance on security controls is based on this special publication 800-53 and 800-171. 800-53 provides security controls produced to protect federal information systems, including access control, auditing, incident response, media protection, business and business recovery. The only draft guidance states that for contract systems, operators on behalf of the federal government, an agency must require the contractor system to meet the appropriate baseline in 800-53 as modified the agency's risk management requirement. Also, for control and classified information or CUI, the modern baseline for confidentiality should be applied and adjusted if necessary. However, for contractors internal systems used to provide a product or service for the government, but continue to propose that the agency should require the contractor to meet their requirements of 800-171 rather than 800-53. Unless 800-171 provides instructions to federal agencies for protecting CUI or non-federal systems and/or limitations where the data is processed or stores transmitted.

On cyber incident reporting, OMB draft guidance provides that reporting requirements are similar for systems operated on behalf of the government and contractor's internal system except that reporting for incidents affecting the latter is required only for CUI.

The guidance states that at a minimum agency contractual language must include, for example, that in the incident of a cyber incident the timeline for reporting to an agency should have information in a report. In every report the guidance says that this reporting will allow the agency and the contractor to work together to investigate the incidents and take other responsive actions.

Persistent security assessments: Contractors are required to ensure certain safeguards are in place before operating a system. The draft guidance also would require agencies to have access to conduct security reviews on a periodic- and event-driven basis for the length of the contract. In addition, is also has verification of security assessment results by an independent third party or the contractor based on the agency's risk assessment.

For security monitoring: The only guidance that relies on the initiative known as Information Security Continuous Monitoring, or ISCM. ISCM is identified in this 63 or the OMB. The guidance states that at a minimum a contractor operating system on behalf of the government must meet or exceed the monitoring requirements in the prior OMB memorandum and that the agency must elect to perform monitoring and heightened security of contract systems with tools and infrastructure of its choosing.

On business due diligence, the draft guidance

notes that GSA has been working with agencies that support and file the use of public records, publicly-available data, and commercial subscription data to support due diligence analysis. The guidance would direct GSA to promote due diligence information sharing service and make research tools available to agencies for these purposes. Slide, please.

On August 26, 2015, the Department of Defense issued a new term rule amending its position regulations. The end term rule implement section under National Defense Organization Act, or and NDOA, for fiscal years 2015 and 2016. The end term rule requires contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on covert systems or on a contractor's facility to provide operation in critical support. The end term rule incorporates security controls from 800-171 stating that it is specifically tailored for use of protecting sensitive information residing in the contract information systems. Slide, please.

DOD's end term rule also establishes policies and reviews when contracting for cloud computing services. For example, the rule provides standard contract language for the inquisition of cloud computing services, including access to computer porting. These requirements work in conjunction with the prior guidance in the acquisition of

commercial cloud services. DOD instruction 8500.01 cyber security outlines all of this. Regarding all vulnerabilities in a D global sources and distribution also states that risk assessment should be addressed as thoroughly as possible in the acquisition of an ID and in an integrated manner across the IT life cycle. The end term rule know that the high-profile cases of federal show, need to ensure information security protections are clearly, effectively, and consistently addressed in contracts. Slide.

In addition, DOD addressed supply chain risk management in 12 instruction 5200.44 on protection of measuring critical function, trusted systems, and networks. DOD instruction 5200.144 requires various heads of DOD components to develop requirements, best practices, and mitigations for trusted systems and networks. The intent of the instructions is to incorporate the framework applicable solicitation and contract language. DOD instruction 5200.44 identified the activities needed to address supply chain risk such as: Reducing vulnerabilities in the DOD system designed for system security engineering, controlling quality; configuration ans security of software, firmware, hardware and systems throughout their life cycles, including components or subcomponents from secondary sources, reducing the

likelihood of unknowingly using products containing counterfeit components, detecting vulnerabilities within custom or commodity hardware and software, and implementing tailored programs for critical components in applicable systems, and implementing an item unique identification for national level traceability and critical components in accordance with DOD instruction 88.20.04. Slide, please.

Since at least 2006 the Department of Energy has been working with various efforts involving cyber security of energy delivery and control. In 2009 DOD, DHS, and industry cyber control systems such as NERC experts elaborated to publish cyber security procurement language control systems. This documents summarizes security principles and controls to consider when designing and procuring controls in product and service. In 2011 the energy sector control systems working group developed a roadmap to achieve energy delivery systems computers. The roadmap includes strategies to help the energy sector efforts. Further, the roadmap states that including member security in the procurement process aligns the strategy to build a culture of security, helping to make cyber security practices reflexive and expectant of energy delivery. In 2014 DOE released cyber security procurement language for energy delivery systems. This documents was developed by energy effective control systems working group on the 2009

procurement document.

The 2014 document contains baseline cyber security procurement language on topics such as affective control account management, session management, and authentication on logging. And the documents also addresses, for example, a private security program which should cover a product's design, development, manufacturer, storage, delivery, and limitations, maintenance and disposal. The document states that properly designed and implemented security programs should lower the risks that the supplier's product will present cyber security challenges for the inquirer. Side, please.

In 2013 the Office of the Comptroller of the Currency issued bulletin 20013-29 providing guidance to national banks's and federal savings institutions, assessing and managing risks with third-party relationships. While this bulletin addressed many aspects of third-party relationships, its guidance under the Commission's theory would include the following recommendations: Assess the third party's security program; determine whether the third party has efficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities; determine whether the technology is necessary or determine and assess the third party's infrastructure application securities

program, including the software development life cycle and vulnerability penetration; evaluate the third party's ability to implement affective, sustainable corrective actions to address deficiencies discovered during testing. Next slide.

The Federal Financial Institutions Examination Council, or FFIEC, includes representatives of the Board of Governors of the Federal Reserve System, the FDIC, the Office of the Comptroller of the currency, and other financial charges. In June 2013 the FFIEC issued a federal security assessment rule to help the Commission identify the risks and determine their cyber security maturity. The tool addressed various aspects of cyber security maturity, including internal management. That role of the baselining controlled several of the baseline controls described; external dependencies provide that. The base due diligence are performed by third parties before contracts are signed, including reviews of their background, reputation, financial position, stability, and security controls. Contracts stipulate that third-party security controls are regularly reviewed and validated by an independent third party and contracts establish responsibility for responding to the securities. The evolving maturity level controls include the following: Critical business processes have been mapped to the supporting external connection;

responsibility for the dedication; direct and indirect security incentives and vulnerabilities, if documented in contracts; and monitoring of third party's scale in terms of depth and frequency according to the risk of the third parties. For the advanced maturity level controls include the following: High risk spenders are conducted on an annual basis; contracts require third-party service provider securities to meet those of the institution; and third-party employee access to confidential data on third-party systems is tracked actively. Slide.

In summary, the federal agency program highlighted in this presentation could be used to inform or help guide the development of a new or modified reliability standard to provide security controls for supply chain or industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. This concludes my presentation of supply chains security efforts by other federal agencies. Thank you.

MR. BARDEE: Thank you, Simon.

Are there any questions for Simon? We'll go ahead and get your presentation on the slide deck posted in e-library. There's a slightly longer version which we shortened a little bit to accommodate the schedule today. Thank you.

If our first set of speakers could now come up, we'd appreciate it. So each of our speakers will be given some time to make some brief opening remarks before we get to questioning. I would just ask the panelists before you speak turn the microphone switch on in front of you; when you're done turn it off, please. With that, I will introduce our first speaker, Nadya Bartol, who is with the Utilities Telecom Council. Nadya, thank you for being here today.

MS. BARTOL: Thank you very much.

Good morning and thank you for the opportunity to participate in this important initiative. My name is Nadya Bartol, I'm vice president of Industry Affairs and Cyber Security Strategists. UTC is a global trade association dedicated to serving critical and infrastructure providers such as electric, gas, and water utilities. My role is to oversee the cyber security initiatives, working with our members on their cyber security challenges. My remarks today are based on my work here regarding cyber supply chain initiatives within the government entity organization since 2008. My remarks are also based on my experience covering as the project editor of the first and only comprehensive global standard of information security relationship.

ISO supply chains has emerged as a challenge

relatively recently. The electric utility comes to this challenge well-served by a comprehensive set of list of studies that addresses cyber supply chain standards relating to the supply risk chain. While there are many available standards guidelines and best practices, some of them will be discussed here today, and there are more. Before NERC's international prior relationship ISO 670627, an international standard and security requirements for industrial control system's providers, RET6243-4, an international standard that provides guidelines reducing risks contained in my department, I-243, and also UTC's cyber supply chain risk management utilities roadmap for implementation. This is not a full list. I should note that most of these documents, including the ones that will be listed, reference each other and many of them share the same content.

So why are we still challenged and what are the challenges? Cyber supply chain risks evolve continuously and many of the practices and processes to address are implemented within their security ecosystem and across other industries. These challenges include: Influence of the ability of transparency and what happens. In some cities there are problems to assemble, and these are where solutions are being similarly challenged, supply chains. Knowledge of best practice is not uniform across industry.

New ICT companies continue to enter the electrical utility market; some of these companies do not have the background in IT or the knowledge to deliver.

And finally, managing, coordinating, due diligence is very complex. Adding security requirements should be done carefully to reduce risk with construction of the primary delivery of critical products and services, and there's a financial impact to utilities and their customers. NERC CIP 5 standards also covers control of the registered entities. This coverage includes supply personnel with access to the systems and facilities. Examples are detailed in the written statement and include many items from personal risk assessment to best corporate standards. Prior standards encourage the development and implementation of security features such as multi-factorial visitation and unique passwords. We know from our member organization, both utilities and their technology partners, that NERC CIP requirements are the best technology procurement. Solutions that perform in compliance are viewed favorably in the market. However, the current standards do not encourage truly innovative security processes for the quality of techniques that involve beyond NERC CIP requirements. Security risk factors have compliance risk which makes entities reluctant to pursue both procurement and security opportunities.

We believe that FERC should refrain from directing development of a new CIP standard for the reasons articulated above. However, FERC can engage in a number of utilities that could help, specifically FERC's Commission study that would collect, summarize, and make available to the industry existing standards and guidelines. The study would capture the list of existing standards, guidelines, and best practices, as well as thus implementing organization within and outside of the electricity sector; continue encouraging the dialogue on this topic among the suppliers about better solutions; and finally continuing and getting the industry into discussions in a structured format like today and unstructured format such as workshops and facilitated discussions. It's a complex challenge that faces an organization's collective education and collaborative work across the utility ecosystem is required. Thank you.

MR. BARDEE: Thank you, Nadya.

Next we have Jon Boyens. He is from the National Institute of Standards and Technology. Jon?

MR. BOYENS: Thank you.

So I was unable to submit a written statement primary due to anything written necessitates a fairly long time. Please bear with me; I will try to be quick. But I did want to get something down for the record as well.

Good morning. I'm Jon Boyens with the National Institute of Standards and Technology and leader information and communication technology supply chain risk management program. Thank you for the opportunity to participate in this event. My remarks this morning represent my own opinions; they do not necessarily represent those of my agency. I will do my best to respond to the four bulleted areas of interest in the agenda, but not necessarily in that order, based on my experience over the last several years. But I must provide the caveat that my research guidance work of ICT or cyber supply chain risk management, I will use those interchangeably, and it does cover both information technology and operational technology. I've been directed through federal government organization to provide a high level of cutting across multiple sectors, but my work is not focused specifically on the energy sector. Over the last decade supply chains have become increasingly dispersed, efficient, and globalized. Improved supply chains, together with pre-trade policies, have offered remarkably benefits to the ICT industry who build employ products and services. These advantages have benefited both public and private sectors for society at large by making affordable and innovative products and services available. However, this trend has also created a complex system in which it is difficult for

suppliers and vendors in the like to understand or control the often-opaque practices and processes used to design, make, source, and deliver products. This in turn makes it difficult for organizations to understand how to mitigate to their supply chain, as well as risks to the products and components traversing their supply chain. And while supply chain risks may exist for all products and services, the lack of visibility and control that an end user has with respect to quality, integrity, ans security products and services compounds the challenges of effectively managing these risks.

Due to the complexity arising, it is often difficult for inquirers to make any informed risk-based purchasing decisions. In many respects technology evolution has outpaced procurement practices. User demand for better, faster, and more broadly-applicable capabilities frequently takes precedence over the demand for security. As a result, ICT functionality reasonably expresses the development of acquisition practices that may not be secure.

Traditionally, ICT risks have been managed within the cyber security or information security domain, while supply chain risk management has remained as a separate focal area. ICT and compliance risk management lies -- and that's ICT or cyber supply chain risk

management -- lies at the intersection of cyber security and supply chain risk management, mixing risk and mitigation strategies from both disciplines. However, in many organizations cyber security and supply chain risk management are considered separate; their management processes often operate in isolation or do not intersect. This disconnect often prevents an organization from clearly defining its internal roles and functions, fully using their existing capabilities and tools, or from expressing and negotiating expectations externally through agreements through partners both upstream and downstream.

If taken to one extreme, ICT supply chain risk management could conceivably encompass all elements of cyber security such as covering the entire system development life cycle. On the other hand, if ICT supply chain risk management is very narrowly defined, such that it encompasses only logistics and related activities, gaps in areas such as security-of-design manufacturing and quality assurance will render even the most rigorous, innovative logistic core process ineffective. I would state that the opposite is true, too, that if it's only focused on information security, much is lost.

The approach taken by NIST in its recently-released social publication 801.61 -- 171 -- 161, supply chain risk management practices with federal

information systems organizations is to address ICT supply chain risk management in a manner previously unaddressed by either traditional information security or supply chain practices. NIST's work and ITC supply chain risk management dates back to 2008 when it was asked to develop guidance for federal agency's nonnational security systems. NIST spent the following three years doing research and engaging with government and industry stakeholders to develop notional guidance. Though we released this notional guidance as a NIST agency report or a NIST OIR, which in this instance is best characterized as the white paper, NIST chose to take a different approach when it eventually offered more formal supply chain risk management guidance in federal agencies. This decision was made after a consultation with industry and government stakeholders, and based on the fact that our notional guidance recommended unique practices that diverged from existing requirements, and would have been too costly for federal acquirers who ultimately had to bear the cost for implementation.

As the information security controls by themselves were being insufficient for managing supply chain risk, the approach NIST took was publication 800.161 was to integrate supply chain risk management into and build on existing NIST guidance in security control,

supporting risk management activities. This approach provides acquirers of supply chain risk management with specific guidance and controls while minimizing the burden to suppliers. While this approach may not be perfect, as it still may over-live or rely on information security control and not fully integrate information security in traditional supply chain risk management, it allows organizations to develop policies and practices commensurate with the level of risk.

Though ICT supply chain risk management remains an embryonic discipline with diverse perspectives on foundational definitions and scope, incomplete, shared, and understood bodies of knowledge and fragmented approaches of standards of risk practices, many organizations -- many who are here today and will be speaking later -- including owners and operators and IT vendors, nonetheless use sophisticated, proprietary practices. Stemming from the work necessitated while developing the framework for improving the framework around critical infrastructure cyber security is the leading research on industry best practices for cyber supply chain risk management. Though this research is not yet complete, our finding that some best practices ranging from organizational strategies that break down functional loads to vendor risk assessment framework and assessment tools, to manufacturing quality

and integrity, and many, many more.

While I shared NIST's approach with what I hope constitutes lessons learned, I would also FERC to continue to broadly engage all stakeholders, as well as the broader ICT supply chain risk management community across all sectors to find the best approach and solutions to what is undoubtedly one of the most difficult challenges we face today. Thank you again for allowing me to address this important topic.

In short -- in summary, I should say -- while I do not believe information security controls are sufficient to handle the broader supply chain issue, that it's important to be flexible and non-prescriptive, or the burden of many of those controls are both placed on the acquirer as well as the supplier.

MR. BARDEE: Thank you, Jon.

Next we have John Galloway with ISO New England.

MR. GALLOWAY: Good morning. My name is John Galloway, I work at ISO New England as the director of cyber security. I'd like to thank the Commission for setting up this conference to discuss the issues related to supply chain risk management and providing me with an opportunity to speak.

In sum, ISO New England supports the Commission's proposal to direct NERC to develop

requirements relating to supply chain risk management. We believe the risks the reliability of the bulk electric system that result from compromised third-part software are significant and largely unaddressed by existing reliability standards. A new reliability standard that requires vendors to test their use of best practices is the best and simplest way to reduce these risks. While many public utilities are already addressing these risks and asking vendors to address, these one-off efforts are less likely to be effective than an industry-wide reliability standard.

In my next comments I'll try to direct the rest of the issue before the Commission. Challenges faced in managing supply chain risk: One challenge that comes up immediately is the number of possible risks one were to simply try to enumerate them, multiplied by the number of supply chain members which may or may not be obvious depending upon how well one can remain transparent into how supply chains act or form. Absence of current security: Quality assurance practices in some supplier cases poses a bit of a challenge; for example, some software suppliers. These notions are new to a few companies that may be in the midst of trying to adopt such practices, while in the case of a well-established or larger software provider like Microsoft, these practices have been standard for years. So there's going to be diverse adoption in some cases.

Another challenge: Required to buy or build risk tradeoffs are going to be part of regular project practice. And that goes hand in hand with development of contract purchasing. If you add supply chain risk, that changes culture with take quite awhile to actually work their way through an organization.

Effective evaluation of the enumerated risks or prioritization in business decision-making such as vendor selection and rating practices: That's an awful, big mouthful. But basically changing such practices takes time; people have built up experience for years in that sort of effort and this would require a re-thinkable lot of the way that's done. A number of vendors may chose not to negotiate further contract terms for their security postures, especially large vendors. Attempts to get a contract for protection would be difficult, thereby having a reliability standard would increase the likelihood of success if all of the entities in the industry need these same protections from these vendors.

Point 2: How the current CIP standards provide supply chain risk management control today. Version 5 of CIP 3, 4, and 5 already address logical and physical controls for onsite vendors. In addition to Version 5, 6 and 7 require systems security management controls for software supply for supporting reliability functions.

However, these existing reliability standards are far less comprehensive than we need. They are precedents for NERC standards and they require a registered entity to manage their relationship with their vendors, so they contribute in some sense to mitigating current supply chain risk, but there's more that can be done.

How the current CIP standards incentivize or inhibit introduction of more secure technology. In terms of incentive, the existence of the reliability standard for some years now has promoted discussion of cyber security requirements for products and practices relative to reliability functions. And this is simplified and supported in negotiation of contract terms for qualities of software being purchased, as well as the support for such systems. So there's already a good track record indicating that such standards could possibly influence supply chain risk mitigation. In terms of inhibition, there are some assumptions built into the present standard requirements regarding network and physical citing and access restrictions that may make adoption to some technical measures permitting reliability function more difficult. Specifically, recent advances in virtual networks, virtual storage, virtual systems, and application clustering which can support a very dynamic provision of the services and improve availability or resilience, may result in multiple,

physical, and network locations being involved. This can pose a challenge when one's looking at a standard that looks to have services identified specifically in particular electronic or physical security parameters. So compliance risk can be part of the picture when implementing the more-advanced form of service.

Possible other approaches that the Commission can take to mitigate supply chain risk: The Commission could work with industry, Department of Energy, and NIST to update the cyber security framework to include or further specify consideration in the use of supply chain risk management in that standard. But I would remind you that that framework is voluntary in nature at the moment and does not provide as much support in a contract negotiation as a mandatory reliability standard, if one were approved by the Commission. The Commission could direct NERC and industry to augment or enhance controls currently associated with CIP 7 system management controls relevant to supply chain risk management. This might involve extending CIP 7 standard regarding system security management. This could increase administrative burden and particularly reliability standards which is tended to be scoped in terms of systems quality as a presently-given entity, as opposed to those being developed along the supply chain. This would be an indirect, and perhaps not

as well-understood, approach to the industry as compared to the reliability standard directly addressing management supply chain risks. Thank you, that's my comments.

MR. BARDEE: Thank you, John.

Next we have John Goode from the Mid Continent ISO.

MR. GOODE: Thank you very much and good morning. MISO Mid Continent system operator welcomes the invitation to present a presentation on supply chain security. For those of you who don't know me, I'm John Goode, MISO's chief information officer. I'm responsible for IT's strategy, operations, including cyber security and CIP compliance. I've been fortunate enough to have a long career in a variety of regulation industries, including telecommunications, ample markets and trading, healthcare, and now the bulk electricity proceedings, which I'm delighted to be in, by the way.

MISO's position on supply chain security can be summarized in the following brief comments: MISO supports supply chain security guidance or standards for the electricity industry; I'll emphasize "guidance". Common guidance or standards will establish a consistent baseline across all parts of the electronic industry, which is a good thing. To accelerate adoption in a program, we believe the industry should use prior proven frameworks for

supply chain security, such as those used in the financial or healthcare industry. A unique industry-specific standard may lead to slower delayed adoption; may drive critical vendors out of the electricity industry; and much can be learned from this high trust; and even the independent third-party review used in 16 systems. These security frameworks should be risk based, not necessarily one size fits all.

And finally, CIP regulation on supply chain security should begin with a pilot based on mandatory guidance that we can gauge adoption and effectiveness, as well as create an effective approach to review, including audit, evidence collection, jurisdiction, and enforcement. ISO, like any regional transmission organization, is unique with its relationship to the bulk electricity system. You see our roles providing technology bases with a mission to serve and ensure reliability, versus directly controlling the bulk electricity grid.

Our supply chain's extensive and include some of the most highest technology from biggest vendors in the world, including AT&T, Cisco, IBM, Oracle, HP, Microsoft. As an RTO, ISO has taken an enterprise-risk management approach managing our business, our technology in essence, and our supply chain. With respect to CIP, we have new compliance to CIP standards at a minimum requirement. We

are continuing seeking traditional security standards and best practices above and beyond those required through CIP compliance. For example, the MISO supply chain security program best practices proved to be affective in the financial industry.

When asked what are the challenges in managing supply chain risk, vendors with an ISO supply chain are both numerous and diverse. Within the ESP we have several hundred. As I mentioned, ISO works with enterprise-classed vendors such as Cisco, HP, Oracle, Microsoft, and others, as well as electric industry-specific vendors such as GD Grid and ODTI, just to name a few. Enterprise-classed vendors tend to provide exceptional service, follow well-vetted security standards and best practice. The enterprise-class vendors had already been required to advance their security capabilities and to ensure their security is in a compliance posture for their customers.

We believe vendors that strictly serve the electricity industry are in greater need of supply chain security improvement due to the electricity industry's growing state of security. When asked do the current CIP standards cover supply chain risk management? Current CIP standards address the obligation to register entities subject to the Commission jurisdiction such as MISO. CIP oversees how we design, build, operate, and maintain our

CIP standards, and we enjoy that partnership. These standards do not directly impose obligations on industry supply chain vendors or suppliers; that's left to the registered entities themselves, contract terms or other means, sometimes with great effectiveness and sometimes with limited effectiveness. Additionally, the current CIP standards do not address the upstream development delivery system assigns modifications by these same vendors.

Does CIP incentivize or inhibit or secure technology? Standards create a minimum baseline security that work for the industry; it's a practice we recommend and support. As I previously mentioned with any CIP standard, current or future, ISO will continue to supplement the security standards and best practices beyond those required for CIP compliance to ensure we maintain a comprehensive security program and supply chain security posture.

So to reiterate my position, or MISO's position, we support supply chain security guidance for standards for the electricity industry. We would like to see it based on proven best practice that exist in other industries already, going as far as to directly adopt high trust during other existing framework. These security frameworks should be risk-based, not necessarily one size fit all. Enterprise-class vendors, or first of all industry vendors,

require different controls and different focus.

Finally, again, CIP regulation of supply chain should begin with a pilot based on mandatory guidance so we can gauge its application and effectiveness as a group and create as a group an affective approach to review, including audit, collection, jurisdiction, and therefore enforcement. I have further detailed comments in my written comments. I thank you for the ability to participate in the conference.

MR. BARDEE: Thank you, Mr. Goode.

Next we have Barry Lawson from the National Rural Electric Cooperative Association.

MR. LAWSON: Thank you.

Good morning members of the Commission and the Commission staff. NRECA appreciates the opportunity to participate in today's conference, and we also appreciate that the Commission invited one of our members, Robert McClanahan, from Arkansas Electric Cooperative to also participate on panel 3. So we appreciate that addition as well.

NRECA and its members actively participate in the American standards process including the CIP standards that are today's topic of discussion. More specifically, we had three G&T members, Generation and Transmission cooperative members, that were members or are members of

the current CIP standard's drafting team. We also had many other cooperators that participated by submitting comments and casting ballots.

NRECA understands the importance of the supply chain issue and its potential impacts it could have on BES reliability. We also recognize the risks and realize the dynamic nature of the supply the chain landscape. NRECA and its members do not believe that additional incentives or new standard requirements are needed to address supply chain risks; it's already in our collective best interest to pursue as much assurance as possible from vendors, suppliers, and manufacturers as it relates to adherence to contract terms and manufacturing specifications. NRECA and its members are unaware of any BES reliability events that have been caused by an exploited supply chain risk, and we do not believe there are unaddressed reliability gaps in this area.

NRECA's members already work closely with each other on supply chain issues; they also work together on contract and purchasing best practices, and when practical they work together to increase their purchasing power. Primarily due to them being smaller than many other utilities, it's sometimes beneficial to band together for purchasing needs. The members that we have are also working closely with vendors, suppliers, and manufacturers

to share ideas and increase the understanding of industry needs in the supply chain area. The introduction of new standard requirements addressing supply chain issues we believe could very likely have significant negative impacts on NRECA members, vendors, suppliers, and manufacturer relationship and negotiation strategies.

Further, the introduction of standard requirements could limit the number of vendors, suppliers, and manufacturers that are able and/or willing to manufacture materials in systems for use by NRECA's members and other utilities. This could result in unintended consequences such as quality and price increases and reducing manufacturing capacity due to a smaller pool of entities to buy from. And therefore we believe FERC should refrain from impacting industry, economic purchasing and business strategy practices and decision-making.

NRECA views CIP Version 5 as striking the right balance between specific and prescriptive requirements and providing entities the flexibility to determine the best methods for how to achieve compliance and for a secure and reliability BES. Version 5 provides a comprehensive structure or framework that enables entities to prepare for and adapt to new and evolving threats. This risk-based approach allows entities to quickly adjust their security protocols without having to develop a new standard

requirement for each and every new risk that is identified.

Additionally, as you've heard from some of the other panelists already, we believe that Version 5 standards do address some of the supply chain issues that are being talked about today. The NERC CIP standards are not the only vehicle for addressing supply chain issues. There are numerous supply chain tools and best practices that are in use by industry; some of these include the NIST publications that we've already heard about; also the Department of Energy's cyber security procurement language for energy delivery systems document. And I'm going to plug NRECA here: We also have a guide for developing a cyber security and risk mitigation plan that has been shared with all of our electric coop members.

So, when you look at all of these tools that are out there today -- and there are many more that I have not mentioned -- but there's also internal utility supply chain policies and procedures that have been developed over the decades. This is not an issue that has been ignored; it is an issue that we are all very aware of and we know that it's a changing landscape but we're trying to change along with those changes that are taking place.

In conclusion, NRECA believes that FERC could best help industry by working collaboratively with us, the Electricity Subsector Coordinating Council, NERC, other

federal government agencies, vendors, suppliers, manufacturers, and others, to review and update, as needed, existing guidance tools and best practices on supply chain issues. This, to us, seems to be the best direction to pursue now instead of developing new standard requirements. As an aside, if the Commission were to consider doing such a collaborative process on developing business practices and guidance, I want to let you know we have excellent conference facilities at NRECA in Arlington.

(Laughter)

And we'd be more than happy to host an event like that, which my co-ord said that would help me in. But we would be more than happy to host an event or multiple events like that. Anyways, I look forward to the discussion. Thank you.

MR. BARDEE: Thank you, Barry. We certainly appreciate the offer.

(Laughter)

Next we have Helen Nalley from the Southern Company.

MS. NALLEY: Good morning. I'm Helen Nalley. I'm the operations and compliance director at Southern Company at Birmingham, Alabama. I'm privileged to represent both the Edison Electric entity today, as well as Southern Company.

While we agree that supply chain risks require careful consideration in managing critical infrastructure protection and cyber security, we do not agree that a reliability gap exists in the mandatory cyber security standards CIP Version 5 to explicitly address supply chain risks. Without time and experience from the implementation process for CIP Version 5, it is premature to conclude these requirements contain any reliability gaps that merit formal review int he standards development process. Instead of a directive or additional mandatory requirements, we believe that several existing supply chain practices and procedures provide a strong portfolio for addressing the rifts, including for example the NIST framework as we heard today. Today's conference will highlight several of those practices. This approach is justified and will meet the Commission's objectives because CIP Version 5 standards provide a strong framework that (1) Provides a defense-in-depth or risk-based approach to ensure application of the broad range of security controls proportionate to the risk faced by each company; (2) Allows companies to adopt their risk management strategies as new threats arise and technologies evolve; and (3) helps ensure companies can efficiently integrate the NERC-related compliance action with their enterprise-wide risk management efforts.

Industry implementation of this framework requires comprehensive, highly detailed, and candid discussion and negotiations with third-party vendors on a broad range of sensitive matters within the supply chain. We urge the Commission to recognize its jurisdictional responsibilities and boundaries and consider how most effectively to use them. The complexities of supply chain management both internally, within corporate boundaries, and externally through the business relationships companies maintain with their hardware and software vendors, and the risk-based nature of supply chain risk management practices, simply do not offer a good fit with Commission-approved reliability standards. Moreover, prescriptive mandatory standards may result in the unintended consequences of hampering utility efforts to manage their supply chain risks.

Electric companies take very seriously their public service responsibilities and have strong incentives to maintain high levels of service quality, including bulk system reliability, under a broad range of federal, state, and local requirements. Industrial control system suppliers operate in an extremely large and dynamic global marketplace and incorporate strong processes to protect against intentional and inadvertent assertion of devices of corporate code that can manage or destroy the entity's

assets controlled by information technology components.

In response to the issues, this panel was encouraged to address I'll start with the challenges to managing supply chain risks. EER and other companies experience three broad categories of challenges. First, the market for the hardware and software used in industrial control systems is enormous, global, extremely complex, and maintains a fast pace of technology change. Vendors and users specify and purchase hardware and software systems, all of which include numerous components and subcomponents which may be made by different manufacturers in different parts of the world. The buyers of these systems often do not have full visibility into the complex vendor environment, making management managing measurable system purchases of the supply chain management difficult for users such as utilities. Second, given the diverse nature of utility asset and asset configurations, we need flexibility to choose products that support our specific risk management strategies and meet the functional needs of the system; explicit mandatory requirements cannot provide this flexibility. Third, we have already dedicated extensive management time and attention to dealing with software and hardware upgrades and security patches to vendor-provided systems. In other agencies such as the automotive industry, when vulnerability is discovered in a

vendor's product, it is the vendor's responsibility to remediate it at no cost to the customer, often through a recall process. With utility-control systems there is no obligation for vendor's vulnerability and the customers usually have to pay a maintenance contract for the privileges of obtaining fixes to the vendor's original problem. At times very expensive upgrades to new versions are required.

This supply chain challenge is also regulated under CIP V 5 which brings me to the second issue on how the CIP figure provides supply chain risk management controls. In the joint trade association comments filed with this docket we map the V 5 requirements to the NIST framework to the supply chain control. For example, CIP 10-2 addressed the prevention and detection of unauthorized changes to the BES cyber systems, configuration change management, and vulnerability assessment requirements and support of protecting BES cyber systems from compromises that could lead to mis-operation or instability. So CIP 10-2 requires configuration testing and change monitoring, as well as vulnerability assessments. In addition, both CIP V 4, access management controls for both physical and logical, as well as CIP 11, information protection controls, provide further examples of the comprehensive, in-depth design of NERC CIP standards. The CIP

requirements provide strong incentives for utilities to work with suppliers and vendors during their acquisition, delivery, and integration stages of the supply chain life cycle to minimize their compliance risk during their operations change.

While CIP maps to NIST, it is important to recognize that CIP is not formal for ordinance requirements and compliance obligations. While NIST offers a broad range of considerations that companies could consider in developing specific standards, we view a high and rising likelihood that mandatory requirements in technology and inventions affixes flexibility for tailoring IT strategies and designs. Specifically, we are discovering that CIP Version 5 implementation has created some significant challenges for the use of innovative security solutions.

And as mentioned earlier, for example, CIP Version 5 is silent on virtualization, a technology not contemplated at the time the Version 5 standards were drafted. Without clarity for demonstrating compliance, companies could seek technology applications that allow more straight-forward compliance demonstrations. This issue can become more troublesome if the Commission required additional mandatory requirements to address supply chain risks.

In addition to inhibiting flexible technology

designs and using new technologies, additional mandatory supply chain requirements will likely hamper negotiations with numerous vendors and could possibly discourage vendors from entering or remaining in the market to serve the utility industry. We strongly believe that requirements will ultimately narrow the market field to only the largest vendors with the most resources, thus stifling innovation, competition, and potentially increasing costs. Instead of ordering the developing opening requirements, we urge the Commission on ensuring that the CIP Version 5 requirements set an enduring framework that allow utilities to ensure they achieve reliability objectives, including cyber security risk management, and allow for flexibility in deciding how best to efficiently and effectively achieve those outcomes and manage the risks. Companies do not lack incentives for maintaining reliability.

I appreciate the opportunity to represent the EEI members and Southern Company and I look forward to further discussion.

MR. BARDEE: Thank you, Helen.

Next we have Jacob Olcott from BitSight Technologies.

MR. OLCOTT: Good morning Commissioners, staff, and fellow attendees. Me name is Jake Olcott, I'm going to share some observations with you today on this topic of

supply chain risk management. I have spent more than a decade working on cyber security, legal, and policy issues affecting the electric grid and other prevalent structures, including on the supply chain security. I was a lawyer for the House of Representatives Homeland Security Committee, as well as the Southern College Committee. I am now currently vice president with BitSight Technologies.

In brief, BitSight is a cyber security information company. We rate companies based on security incidents and configurations we observe from entirely outside from their networks. Our ratings and underlying data provide our customers with quantitative, objective, real-time information about the cyber security posture about their third- and fourth-party supply chain vendors and partners. BitSight is currently rating 40,000 organizations, including over 2,000 energy utility companies and thousands of their critical third-party vendors. A number of our customers are testifying today.

In the interest of time, I'd like to highlight just a few informations from my written statement. First, cyber tech targeting and supply issuing have become very common, particularly attacks against third-party business associates and third-party service providers. Sometimes these parties have a direct network connection to the first-party network, and this was the case in the attack

against the retail vendor, retail chain, Target, which actually began with an attack against Target third-party vendors; the malicious actors essentially wrote a connection into the Target network.

In other situations the attackers target a third-party business that does not have a direct network connection but still holds a lot of sensitive data. This is the case a few months ago in the example of T-Mobile where T-Mobile customer accounts were stolen and the malicious actors wrote into Experian, which is a third-party business associate of T-Mobile, also affecting many of us current and former U.S. government employees and their background check information where the malicious actors broke into third-party contractors to the federal government to steal background check data and also credentials. As already suggested, the electric sector is not immune from these challenges and these types of attacks, and third-party utilities have been targeted. Bitsight regularly observes security maintained on a variety of electric sector organizations, including third-party vendors. As more organizations focus on protecting themselves, the malicious actors will continue to target weak links, and then the supply chain.

Second, the FERC staff has amended a number of federal and state regulators and other sectors, including

the financial sector, healthcare, retail, consumer data, and others have recognized that third-party risk management is a critical issue for their sectors. And they have established or are establishing regulations or requirements for supply chain risk management. And I just wanted to share some observations with you on those requirements. There's actually a lot of consistency with the way that other regulators approach supply chain regulations.

In short, regulators generally require their regulated entities to create vendor risk management programs that include four main elements: First, regulators are requiring their regulated entities to tier vendors based on totality. This should be treated as a risk-nature approach; not all vendors should be considered equal, some pose a more serious risk than others. Sometimes regulators specify what data should be considered critical, in other sectors it would be personal health information or personal-identifiable information, but also what types of technologies service providers consider critical. For example, in the financial sector it is retail payment systems. The bulk power system's critical third-party may include vendors who provide IT, ICT, and ICS systems critical to the operation's bulk power system or maintain connectivity or access to critical bulk power system networks. But critical third parties may also be

those vendors who hold or maintain sensitive bulk power system data but do not have direct connections into the infrastructure itself.

No. 2, other regulators are stressing that the risk in securing critical vendors should be assessed prior to a contracting award. This is now sort of colloquially -- you know what I'm trying to say -- this is known as cyber due diligence. Organizations will develop their own requirements, they will review documentations, including audits and assessments conducted by any third parties prior to issuing a contractor award.

No. 3, the number 3 thing that regulators are doing, they are requiring that contracts include security provisions. Contracts with critical vendors should include provisions that establish expectations, insurance coverage, compliance with best practices, and timely notification in the event of an incident. As other panelists have pointed out, there are people out there that organizations will ask their vendors to meet, including ISO, NIST, and critical security control technology, trust technology provider standard, et cetera.

The last thing, No. 4, is that regulators ask their organizations to perform what's called ongoing monitoring for the duration of the relationship; And in my opinion this is where the market is really responding to

demands of commercial companies. Previously, the state of the art for ongoing monitoring was the time and mutual intent of the process involving written surveys, onsite visits, and periodic security scans. Organizations and their regulators realize now that cyberspace, where threats evolve on an hourly basis or even a minute-by-minute basis, annual assessments and written responses only provide a snapshot in time. What organizations are interested in are continuous monitoring of their critical vendors. And this is why the National Science Foundation awarded BitSight a prestigious grant in 2011 to work on our field across -- various regulated and unregulated industries are using our ratings today, because we are able to provide a continuous, automated, objective measurement of security performance without the use of questionnaires or intrusive network testing.

In sum, as FERC considers adopting new supply chain risk management standards, it is important to emphasize initiatives that are focused on qualitative, continuous risk management rather than subjective, check-the-box compliance activities. And I would also say it's also important to recognize that there is a rapidly developing market for a third-party vendor risk managements solutions, and BitSight is excited to be part of those solutions.

Thank you very much for the invitation to be here today. I look forward to answering your questions.

MR. BARDEE: Thank you, Jake.

And our final speaker on this panel is Marc Sachs from NERC.

MR. SACHS: Saved the best for last.

(Laughter.)

My name is Marc Sachs. I'm the senior vice president and chief security officer at NERC, North American Electric Corporation. I greatly appreciate the opportunity to participate in today's technical conference relating to supply chain risk management.

As we discussed in our filed comments on the revised critical infrastructure protection standards notice for proposed rulemaking, we appreciate the Commission's attention to this issue, and we feel it is vital to the reliability and security of the bulk power system that electricity subsector participants continue focusing on mitigating security risks associated with global supply chain. As the Commission discusses in the NOPR complex supply chain for information and communications technology, as well as industrial control systems, represents significant risks to the bulk power system security, but also provide various opportunities for adversaries to initiate cyber attacks.

I'm going to discuss a little background on my perspective on the globalization. I'll also talk a little bit about the CIP reliability standards as they stand and how they can relate to supply chain. And should the Commission decide to direct NERC to develop additional reliability standards, I'm going to offer just some considerations the Commission might want to be involved in.

Supply chain risk management is certainly not an issue that most of the electric sector faces by itself. It cuts across all industry sectors; it presents challenges for states, for federal governments, private citizens, private business, all of us. For the past couple of decades I have been fortunate to serve in multiple positions in the federal government private sector in security; I worked a lot in supply chain issues, I've done a lot of research into it. So I can offer a kind of interesting perspective on what we're looking at and the challenges that we're facing. Based on these experiences, I'm aware of the challenges associated with the supply chain risk management in its accordance to the critical infrastructure sectors. Supply chain risk management is a global, complex issue that is not susceptible to a single, one-size-fits-all approach; we have to stay away from that, this has to be somewhat flexible.

Supply chain information and technology control

systems are long, multi-dimensional: They involve numerous parties in a multitude of countries across the world. Many entities may participate in the development, design, manufacturing, and delivery of a single product purchased by one of our registered entities. For example, it's been estimated that nearly a hundred percent of all the electronic components sold here in the United States -- ranging from consumer smartphones, TV sets, microwave ovens, all the way up to control systems sensors and critical equipment -- the electronics and the electronic components manufacturing largely outside of the United States. That's a fact; that's globalization. Nearly all of this movement ranging from Asia, South/Central America, Middle East manufacturing, is due to lower labor costs in those regions, reliable global high-speed communication networks, relatively low shipping costs, and lower than existing import duties into the United States. We cannot go back, we will not go back to domestic-only production business services. Our nation's economy, as well as the economies of other countries, depends on this globalized supply chain. We must recognize that other countries that are experiencing the same vulnerabilities and the same concerns look to the United State for leadership and guidance to help them mitigate these same types of threats.

So let me turn a little bit internal now into

NERC. The supply chain management risks are constantly evolving. The development and sharing of industry best practices lessons learned and developing the technical means to mitigate those risks, including identifying counterfeit or non-genuine components, is the way ahead. NERC understands that the electric industry is already well-engaged in this activity; for example, as already pointed out earlier that we've been participating in development of the BOB guidelines, cyber security procurement language, furnishing delivery systems, EEI as mentioned has already been involved in developing principles and recommendations, as has several others throughout the sector. NERC is committed to using its committee reliability tools, the guidelines, training exercises, situational awareness, what we do with the EEI sec, what is necessary with the reliability standards, to support the industry's efforts to mitigate supply chain risks.

As we detailed in our NOPR comments, our CIP reliability standards already include requirements that help mitigate supply chain risk. Let me just highlight a couple of these; it's a fairly long list. I made these corresponding controls in NIST's SPE protection, which was just been mentioned a moment ago. For example, we have requirements to implement cyber security awareness

programs; to implement personnel risk assessments; to implement access management and access revocation programs; to implement protections to control electronic -- bulk electric system cyber systems; to implement patch management processes; to implement processes to deploy and detect and mitigate malicious code; to implement processes for system access control; to implement security plans; to implement plans to recover the reliability of functions performed by bulk electric cyber systems in the event of an incident; to perform vulnerability assessments; to implement plans to address risks associated with transient devices; and to implement processes for protecting critical information. That's just a highlight; there's many more we could pull from the standards.

But given the limitations of Section 215 of the Federal Power Act, additional NERC reliability standards may not be the most efficient and effective way of mitigating these emerging risks. As the Commission recognizes, the reliability standard under Section 215 of the Federal Power Act has limited applicability. It cannot -- and I'm quoting -- "Directly impose obligations on suppliers, vendors, or other entities that provide products or services to registered entities", unquote. Many of the actions of suppliers, vendors, and third parties are beyond the control of registered entities, and

in turn they breach NERC's reliability standards. To mitigate supply chain security risks, the electric sector participants must work closely with other industry sectors and global partners and the suppliers of these services, and continue to develop, share, and refine existing guidance documents and practices for addressing the supply chain risk management.

However -- this will be the last part I'd like to talk about -- should the Commission direct NERC to develop commissional mandatory standards, let me offer some considerations. First, it should provide sufficient time for standard development activities to enable NERC to thoroughly consider these issues and engage in educational outreach efforts, including additional technical conferences and a formation of a task force, as we discussed in our opening comments, to provide a better understanding of the nature of supply chain risks to the extent to a manner in which mandatory reliability standards can effectively protect against those risks. We also recommend that FERC should clarify that any such reliability standard builds on existing protections in the CIP reliability standards in the practices of the registered entities, and focuses primarily on those procedural controls registered entities reasonably be expected to implement during the procurement of the policy

services associated with bulk electric-sector operations.

As be discussed in our comments, the supply chain management reliability standards could include procedural controls; I've uploaded three areas here: Procedural controls surrounding the need to transact with an organizations that insert criteria, in other words, we would only transact with a trusted supplier; we may include cyber security procurement language in contracts with suppliers, vendors, and contractors for products and services; or we could review and validate security practices with buyers, vendors, and contractors to the extent possible. Another potential approach would be to require registered entities to obtain certification from a supplier that an independent third party has reviewed and endorsed that the supplier's supply chain practices are in line.

Further, the Commission should also stress supply chain management reliability standard, should we develop one, must be flexible to account for the vendor's need with registered entities the diversity of our system requirements, environments, technologies, and risks, and also the issues related to developing these mandatory NERC reliability standards.

I thank you very much for the opportunity to present these issues. I look forward to any questions.

MR. BARDEE: Thank you, Marc.

Given the time left for questioning, let me turn first to our Commissioners and see if they would like to ask any questions before staff does. If you prefer that staff do the questioning, that's perfectly fine, too.

COMMISSIONER LaFLEUR: I guess I'll ask one question so I don't take all the time.

That was really helpful. I'm sorry I stepped out for a minute, but I did read all of the testimony also. In really struggling whether there's a way that the Commission could add value through our Section 215 work, I take as valid the point that companies are self-motivated to have good supply chain risk management already; that's clearly true. But that in a way proves too much, because that's sort of everything we regulate under the standard. Companies trim trees and set relays and fenced in their substations long before Congress gave us the responsibility to set mandatory guidelines and audit them. So in some ways they're always codifying common steps and being one step ahead.

Several of you have mentioned leveraging, somehow leveraging, the work of ISO, NIST, DOE, the financial sector, other organizations. Could anyone suggest how we should do that? Should we somehow require companies to follow a particular guideline, look for

guidance, look for clarity when we do audits that they're on top of it in some way? Or just put out a guidance document for pointing people in the right direction? Other than finding that there's no reliability gap here, does anyone have any suggestion about what we do with all that work that's been done? Just to keep myself quiet, I'm going to pass the mic along now.

MR. BOYENS: So the two documents, NIST documents that were referenced, are the cyber security framework, which is not a standard, it's a big framework that involves many different standards. Part of our work stemming from that, since supply chain is really mentioned in only one subcategory of the entire core framework, is to look at how supply chain risk management fits into the cyber security framework. Because it really runs throughout all the different functional areas. Now, part of our process, which is not finished, has identified some gaps in that. The second publication, which I led and coauthored, was the 800.161 specifically to supply chain risk management for federal information system and organizations. Our approach that we took there, since it was not deemed that information security controlled by themselves covered aspects of supply chain, but yet we didn't want to be too disruptive. So what we did is we took the current guidance on risk management, the current

guidance on risk assessments, and added in supply chain risk management aspects into those processes.

Similarly, when you go into the control selection, what we did is we extracted -- we looked at over 800 different control enhancements in our security catalog -- extracted those out that we thought were specifically related to supply chain risk management, and then we offered supply chain risk management implementation guidance that is specific to those controls. So instead of trying to create a completely different paradigm, which we did in our initial notional guidance which we pushed back several ages, we decided to use something that was already in place and modified.

COMMISSIONER LaFLEUR: So is it your point that we should look through CIP and see what's already there or we should point people to the NIST documents and say "this has been done"?

MR. BOYENS: So it's outside of my purview to really comment on CIP. But that is one approach, would be to look at what is there and do a gap analysis.

COMMISSIONER LaFLEUR: Thank you.

MR. GOODE: I would like to enter a statement in response to the Commissioner. I think we could look at existing work that's been done to very quickly identify frameworks that are applicable as a base of mandatory or

voluntary guidance, right. Voluntary guidance, then you could actually do reviews if you wanted to if our regions go out and do reviews of everyone's acceptance and driving efficiency of that. I think there's a big learning opportunity for us; there's work that's gone out already, supply chain is very broad, very close, right. And we want to get the things that actually increase the cyber security protection of the grid and not just wind up being a reporting obligation, right. So, again, I think we can pull together as an industry group working with FERC and NERC, identify the standards we want to follow immediately, start the education and the training within our organizations to make sure we're following those standards. And then much like the SEC, which was somewhat voluntary, ISO would be welcome to review by their regions to make sure and assess our cyber compliance, our voluntary compliance of that standard.

MR. LAWSON: Yes. I think we have to remember that the Department of Energy developed a very focused set of best practices on supply chain issues for the electric utility industry. Maybe that's a good starting point. We don't need to develop something new if we have something that is already very focused on our sector. And I believe that that document takes into account many of the other documents we've heard about today. Let's take a look at

that collaboratively, like I mentioned earlier all players, let's look at that. Let's see if updates may be needed; if they are, let's work through the Department of Energy to update that. Let's see if anything more than that might be needed. The thing is it's already there; let's see if there's anything that needs to be modified.

COMMISSIONER LaFLEUR: But you would keep it modified?

MR. LAWSON: Yes.

COMMISSIONER LaFLEUR: Not somehow incorporate the DOE standards is what you're saying?

MR. LAWSON: Yes.

MS. NALLEY: I was thinking about this, that we already have an excellent example of how to do this in a collaborative way with the risk-based compliance monitoring enforcement program. NERC, along with regions and industry, and I was one of those participants somewhat in that process, have really moved the compliance monitoring enforcement program light years in that process. And I think that kind of collaborative approach that isn't a mandatory standard, that is a practice that the regions can utilize in their compliance programs in monitoring, and I think that's an excellent example of a process we could use to take this forward.

COMMISSIONER CLARK: Thanks to everyone for

excellent comments. If I were to give an overview of what I think I've heard, which is the first question of: Is this important and are the potential gaps here in something we need to be paying attention to? This is something we all need to be paying attention to, number one. So that's good, we all got agreement on that. Once you move past that to the question of should there be some sort of FERC/NERC standard or not, then it's fallen into two camps. One is, yes, it's important enough to merit a standard. But within that, the next thing I sense strong anonymity that it needs to be flexible, it needs to be risk-based, not prescriptive. The other argument would be no, it would be better to have voluntary standards in an industry inceptive to do the right thing in this case. It's interesting, I had the exact same reaction that Commissioner LaFleur did, which is: The Commission can't just rely on that argument. Because if we rely on that argument it calls for the question why do we have CIP 1, 2, 3, 4, 5, 6? That alone, I don't think would be enough because it's kind of a pre-215 world for the Commission.

So then we have to ask : If voluntary is enough, it would be helpful to know -- and I know some of you have bits of this in your testimony, but if you put a little bit more meat on the bones -- is there something that's different about supply chain management that makes

Commission action in this particularly ineffective or ill-suited in a way that differentiates it from all of the other areas of CIP standards that we've done, and voluntary actions are better or more efficient in this case, but it's somehow different than the last one? So if you could just sort of tease that out for me a little bit, that would be very helpful.

MS. BARTOL: So to the question cyber supply chain risk management is a shared responsibility between acquirers and suppliers. We use the term in that sense, which is from session to disposal, and only a life cycle is within the control of the registered entities. Then you stop with the registered entities could do anything, and then the supplier part of it starts. So there's a jurisdictional challenge and there's only an inference challenge on the part of the supplier and the energy-developing facility that some of things they can influence and some they cannot. So it creates an inherit limitation in the challenge.

COMMISSIONER CLARK: Are some of those challenges overcome by the Commission -- and obviously we can't directly ask the vendors themselves or the suppliers -- but if a standard is written flexibly enough that we're incorporating some of the things I think we talked about in terms of ensuring that you're following

best practices to manage the potential, maybe it's things like third-party oversight or third-party certification when you're dealing with the proper matters, things like that. Or is it not the Commission attempting to write the rule but rather ensuring that the utility is following best practices. Does that ameliorate those issues that we've come to at this point or is there a way to get around that?

MR. GALLOWAY: I believe that that would actually ameliorate some of the difficulties encountered in the complex relationship between the supplier and the provider and user of technology. So at ISO New England we believe that, yes, third-party reviews, due diligence, and just tracking the risk per vendor class and the like would probably serve well enough to mitigate some of the risks that we see regularly in dealing with some of our suppliers, that we just need to see a consistent approach, see a baseline developed for it, and that be something that we know we have to take into every contract negotiation consistently. That's what we're looking for.

COMMISSIONER CLARK: Barry?

MR. LAWSON: I guess I'm looking at this as if I'm a registered entity with NERC. And if there is some type of standard in this area, it has to be understood that we could be talking about me as a registered entity being found in violation of a standard due to something I cannot

control. I don't think that's the way we want to proceed. I cannot control whether a supplier or a subcontractor/supplier providing equipment or devices, software, whatever you want, to the person I've contracted with, but why should I as a registered entity be found in violation of something I can't control in the first place? So, yes, we can put provisions in contracts; we can negotiate all of these types of things we're talking about here. But we cannot make that happen; that's a contractual issue between me and a supplier. So I think it's a little bit of a dangerous edge to be on in that way, and I think we want to make sure that we're not being held accountable for actions we can't control.

MS. NALLEY: I had the pleasure, in quotes, to be involved in negotiations with some fairly large contracts. And one thing we've run up against is just in negotiating those provisions, the companies have their own perspective of how they want to do business. And as we've tried to impose our requirements on those, it can get to be some pretty interesting negotiations between particularly our lawyers and their lawyers. So one thing I would really recommend, as we think about this further, that we do involve folks who know and understand contract law quite well, because the implications to contract law are pretty significant as you're going through this. So one of the

worries I have about the standard is how reactive standards are as opposed to proactive. And I think the virtualization example that we used earlier is a perfect example of how technology really depends on the standards that haven't caught up to it yet. But whatever we do, it need to be very flexible so that innovation is not stifled and companies have the opportunity to contract with companies that can deliver the best services and products for them.

MR. SACHS: Let me just give remarks here. Having worked with this in other sectors in critical infrastructures, procurement is what we're talking about is a business function, it's not an operations piece kind of like maintaining your books, finances, payment of employees, things that are business processes. So we have to be very careful about: Is a business process something that we want to approach regulation on? That being said, our suppliers are the same of what supplies transportation, telecommunications, finance, and many others. The only thing we can't develop something that's just unique to us again because we're globalized. And not only in the U.S. and Canada, but Western Europe, Asia, Africa, we all have to be consistent.

COMMISSIONER CLARK: Thank you. That's all I have.

COMMISSIONER HONORABLE: Mr. Sachs, I'll begin with you.

And I'll ask pointed questions in the interest of time, Mr. Bardee, because I'm on the clock.

(Laughter.)

Thank you all so much. Your comments were very thoughtful and you've brought a wealth of knowledge and expertise and it will be very, very helpful for the Commissioners, I'm certain, but to our advisors and to the FERC staff as well.

Mr. Sachs, I think I had a question for you about your point about you were saying Commission, we really don't need this sort of standard, however, if you decide to go there here are some things to keep in mind. The second point you made is that we should clarify the reliability standard existing protections and focus primarily on those procedural controls that registered entities can reasonably be expected to implement. I want to ask you, you're very courteous, are you saying remember your jurisdictional limitations, you said the point that Mr. Lawson references that be practical and recognize that it wouldn't be prudent to require things of us that are not within our control. I just want to say.

MR. SACHS: I couldn't have said it any better.

COMMISSIONER HONORABLE: Thank you, I just

wanted to make sure we were on the same page. Commissioner Clark's questions regarding verified, I heard that in Ms. Nalley's testimony, thank you for offering that.

My second question is for Mr. Lawson. And first I have to say: Thank you for acknowledging Arkansas. I was looking for Robert McClanahan. There you are. I know you've got a bit at home too. Thank you. And always you are welcome back, in fact the meeting room as you know is the Arkansas coop, I call it the United Nations, it would put this room to shame. So thank you.

I want to ask you, Mr. Lawson, in your comments you referenced, I think you expressed some hesitancy about the need for it in the first instance for this type of standard. And you referenced the potential for significant negative impacts on the working relationship from NRECA's members, manufacturers, within the new standard. Would you expound on that?

MR. LAWSON: Sure. I tried to at least address that quickly in my oral comments. But we're concerned that if there is too rigid of a standard or any sort of mandatory tool in the supply chain area, that you could window down the number of manufacturers, the suppliers, that would be willing to provide such materials and devices to our sector as they may not want to have to work within those parameters. That's one area. I think when you start

getting into the economics of things, we're talking about less suppliers could potentially mean higher prices for this equipment. That means now the Commission could potentially be effectively sitting at the negotiation table with us and our vendors, suppliers, manufacturers. So we're concerned that that has not really been examined closely at all in our sector. And way before anything should be, in our opinion, proposed from the Commission, there's a lot of work and a lot of analysis that needs to be done and considered. So that's what I was getting at.

COMMISSIONER HONORABLE: Certainly. And I will certainly keep that in mind; I'm sure my colleagues will. And particularly the presence, those of you that know me have heard me say this before, our goal is not to allow standards and regulation to impede progress, to impede the important work that occurs in the industry. So I'm very cognizant of barriers and unintended consequences. Thank you all.

Sure, of course.

MR. BOYENS: So as I think to kind of overall: From this experience where we actually developed guidelines for federal agency nonnational security systems for departments and agencies that have very, very broad missions, so we stay at a certain level and offer guidance. But what we found in supply chain risk management is the

key importance for that risk assessment and the risk management approach where you do a criticality analysis to be able to determine where those critical threats are throughout your mission and support your mission. And those threats go down into the acquisition procurement process so that you know where the most important parts and components are where you are willing to actually invest in oral acquisition processes contract language. The second thing which is part of that is we have found that supply chain risk management, which we define as throughout the system development life cycle, really an organization has the most control within its organizational boundary. And many things can be done within that organizational boundary that reduces that risk, that there are limitations when you start going out into the acquisition process in the tier 1, 2, 3 parts of the suppliers. But even in that area we've seen an similar approach between those organizations who has risk, the ultimate risk position, and those making procurement decisions, and that there needs to be a link between those two areas.

COMMISSIONER HONORABLE: Thank you.

MR. BARDEE: Let me ask one question before we excuse the panel and get our lunch break. The discussion so far has made clear there's already been a lot of work done in this area -- no need to reinvent the wheel in this

context -- and also that there's a need for flexibility to avoid unintended consequences and adverse harm to people's business models and needs. So let me turn to you, Marc. I'm open to other panelists addressing this too. One possibility would be for the Commission to say, "Give us a standard that deals with utilities that only deal with vendors who do A, B, C, D", whatever list of controls you might impose on your vendors. Instead of that, would it be preferable, feasible, to develop a standard that says only deal with vendors, at least perhaps for some level of criticality of your services and goods, if they meet a set of standards that's out there. And perhaps NERC could keep a list and update it periodically of a set of standards that would be appropriate in that context, whether it includes things put out by NIST or things put out by other entities, it would just say here's various sets of standards that vendors could meet and whether it's their on attestation or through a third party's verification or through the utility inspection. Would that be one way to build in some flexibility to change this over time and not create too tight a box?

MR. SACHS: I think there are many approaches. We could also recommend the task force so we get a lot of minds together to work on it.

We've seen this in other areas of the supply the

chain, not just ICT electronic-type things, procurement of steel, concrete, building materials. We have lots of national standards suppliers have. So if I'm a road builder and I'm going to rebuild a bridge on I-95, I'm going to build it to a certain code, but the supply system beyond the control infrastructure has been providing me with steel that meets some certain standards. This applies to all suppliers of steel. Could we do that with ICT? Could there be something in place for critical infrastructure that's found in public and private sectors, that those components have to meet some sort of federal standard? That's a possible approach, and certainly would apply to all critical infrastructures and not just electricity. That's my biggest fear, we would develop something that's just for us and it doesn't map to what everybody else is doing. I think that's what you've heard here, we've got a wealth of knowledge that's been accumulating to leverage that system with all the other infrastructures. Because we're all buying from the same suppliers: Same country, same sources.

MR. LAWSON: I think we're better served to examine these issues outside the standard process. As soon as you go into that process, there are certain rules, there are certain -- I guess I'll say it becomes much more legalistic at that point. I think we'd be best served to

do that outside of that process. I think DOE is a very logical place to start. They have a guidance document already very specific to what we're speaking of here today. And I think we'd be best served to do that, starting with DOE. It was a very good process to develop that document; DOE worked very closely with all sectors of the electric power industry, and I think I have no doubt that they would do that again in that kind of work.

MR. GOODE: I believe that that would be an excellent way to start a program and actually accelerate adoption of it. Then you could look at here's a set of framework that factually convey the same guidelines and standards FERC could develop. Your large enterprise vendors that are already compliant to other industries are selling to, to feel free to provide at the stations around that. Smaller vendors who need to billicate [sic] ability to identify a standard and build forms across the several -- the different industries they'd work in, I think it would be good for our suppliers, good for us, and also good for the Commission.

And the final piece of it is we're dealing when it comes to cyber security with very sensitive topics: The whole issue of evidence, how do we prove that our vendors are compliant? And we need some sort of third-party review adoption of the existing standard that potentially provides

that framework would be an excellent way, again, to accelerate adoption, incorporate in a year versus years.

MS. NALLEY: One final request is that we remember the complexity of the bulk electric system and the fact that we have systems that are old and decrepit. I guess I shouldn't use that word, but they're old. And we have systems that are much more new and modern. And so something that is safe and does reflect the differences in the systems that are in place today would be extremely helpful.

MR. BARDEE: I'd like to thank all of you for being here today and, again, apologize for the late start and the adjustment to the schedule. But we certainly appreciate your insights today. I look forward to working with you as this process goes forward. Thanks.

We'll be back at 1:45.

(Whereupon a lunch break is taken.)

MR. BARDEE: Let me welcome back everybody for this afternoon session, starting with panel 2. We had a thorough and interesting discussion this morning, and if the audience will settle down we'll proceed with a little more conversation. I'll just introduce the speakers as we go down the table, we'll start here with Michael Kuberski.

MR. KUBERSKI: Thank you. Good afternoon, Commission staff. I'm Michael Kuberski, I'm the manager of

protection and automation for Pepco Holdings. Thank you for the opportunity to participate in today's technical conference.

Pepco Holdings is one of the largest energy deliver countries in the mid-Atlantic serving about two million customers from Delaware, District of Columbia, Maryland, and New Jersey. Pepco provides regulated electric service, Delmarva Power also provides all -- natural gas. As a service provider for our nation's capital, we recognize our responsibility to employ effective, cost-enrichment plans to maintain the safety and reliability of the nation's electric grid. We respect and share the Commission's goals to focus on the security and reliability of critical infrastructure.

Consistent with Edison Electric Institute and the Joint Trade Association, comments filed in this document, PHI does not believe that a new or modified NERC reliability standard is needed on top of the existing standards to continue to achieve these goals. Primarily, we feel Version 5 of the mandatory NERC CIP, Critical Infrastructure Protection, cyber security standards are reasonable and appropriate and require that will be facilitate risk management. Electric utilities are similar to critical services we provide. However, the utilities do not fit in the one-size-fits-all approach. There are

differences in the operational, information, and communication technology assets we procure to safely and reliably deliver electricity to our several territories.

We find ICTS suppliers are constantly innovating and driving better solutions in the marketplace. Utilities need the flexibility to adapt these solutions. Additional requirements may hinder marketplace advancements if they are not modified fast enough to keep pace with the new technology that comes out with discovered products. We should avoid the scenario where the technology exists that is better for security and reliability, but not unusable because it is not part of the standard or creates compliance risk. We also do not want to drive innovative suppliers from the electric market allowing for attackers to focus on smaller lists of vendors to attempt to attack or exploit.

As previously stated, PHI views the CIP Version 5 requirements at appropriate and reasonable. A risk supply chain compromise that could introduce products with malicious functionality is a cyber security threat and for many reasons not under the control of the utilities or vendors. Therefore, the risk is compromise cannot be fully mitigated. Since PHI uses a number of vendors that use multiple third-party suppliers for components and their technologies, PHI views supply chain risk management as a

shared responsibility that requires collaboration and well-defined expectations. Various government activities can also support that collaboration effort by sharing information on product vulnerabilities.

PHI supports existing NERC CIP Version 5 control which effectively provide utility controls for supply chain risks while not overburdening suppliers. We feel supply chain processes should not be regulated but controlled by the organizations that must govern them to their unique environments. We support ongoing efforts involving voluntary guidelines within industry new supply chain cyber risks and system technologies. PHI believes it can adapt quicker to changing cyber environments that we're able to adopt. Vendors have demonstrated a vested interest to secure manufacturing developments and practices if for no other reason then to protect their name brand and market share. PHI strongly believes it has in place effective processes and qualities where these vendors' practices integrating technologies into critical systems which supports CIP Version 5 requirements. In view of the validation of processes chosen by members of ICP providers takes place when PHI conducts requests for proposals for ICP products and services. PHI strongly recommends that the Commission avoid seeking to incorporate various purchasing practices or policies into the NERC mandatory

requirements. Cyber asset contracts should include terms and conditions that specifically address matters of cyber security while providing audit rights to access vendors' securities to contracts.

PHI believes in truly vetting vendors' practices and supports consideration of these steps of the manufacturing process through design to build to ongoing support. It is important to note that we should not be setting guidelines and should not be setting prescriptive measures so that we do not make relatively impact innovation. PHI supports vendor testing and digital inspectional cyber assets. We encourage security assessments for the frequency based on risk, assessed risks, and critical leverage. PHI and its vendor partners will continue to exercise training, management, and control on cyber asset firmware and software and minimize potential exploitable vulnerabilities. PHI conducts periodic threat and risk assessment to vendors and also conducts advanced risk assessments through third-party experts. Based on the findings of the risk assessment, we determine the methodologies to mitigate the risks. Mitigation methods should be evaluated as a key component to our architectural changes needed to be made.

If it is determined that the standard is required to address supply chain, which we feel is

adequately addressed in the existing NERC CIP Version 5 standard, it would be necessary to include key stakeholders in the development of this standard. FERC should not deploy any standard strategy without being informed input of key stakeholders, vendors of operational technology, ICT equipment facilities, utilities and standards organizations. The new NERC CIP standards to be implemented in April 2016 will provide further incentives for PHI to have control to manage the risk. PHI recommends that the Commission allow CIP Version 5 implementation to inform evaluation of risk standard strength, effectiveness, and not create yet another standard. This will allow PHI and vendors to continue to improve upon industry technical standard and approaches for the IT systems that enable critical business processes with an emphasis on the secure functionality of the hardware devices and software applications. For example, creating internal utility technical review boards to guide such approaches, as well as reach and develop new operational technologies and inform information technologies would be helpful. Vendors should play a key role in the early stages of the supply chain life cycle, and we have to ensure that they are aware of our critical security requirements and the implications of noncompliance or non-conformance.

While the existing NERC standards represent

strong processes in mitigating cyber risks to the bulk electric power system, PHI has concerns that additional standards may stifle market competition and technical innovation. While oversight and collaboration with vendors is necessary and exist today in the form of tested, mature and effective -- PHI does not wish to hinder its supplier relationships or reduce the number of potential vendors in the marketplace with requirements that would cause inefficient or costly outcomes or reduce the company's ability to negotiate with potential vendors.

We support continued industry collaboration, including development and implementation of guidelines that are not prescriptive, and that the existing framework offered by NIST, DOE, and IEEE. Together we can maintain the ability needed to protect our critical systems while staying on the leading edge of technology advancements that enhance the reliability and security of our systems.

Thank you for the opportunity to participate in today's conference I look forward to any further discussions on this important topic.

MR. BARDEE: Thank you, Michael.

Next we have Jonathan Appelbaum from the United Illuminating Company.

MR. APPELBAUM: Thank you.

Good afternoon Commission staff. My name is

Jonathan Appelbaum, I'm the director of the United Illuminating Company. Thank you for the opportunity to participate in today's conference.

UI is a subsidiary Omnilight (phonetic), a distribution company engaged in the purchase, transmission, distribution, and sale of electricity of related to approximately 325,000 residential and industrial, commercial, subject to the mandatory reliability standards, developed and enforced by the North American Reliability Corporation. UI supports the association comments submitted by the Edison Institute, the American Public Power Association, National Cooperative Association, the Electricity Consumers Resource Council, and Large Public Power Council.

In response to the Commission' notice on rulemaking issued last year, I appreciate the Commission holding this conference to continue the discussion. UI acknowledges that there are challenges in managing supply chain risk. We do not believe a reliability standard to a modification to an existing standard addresses quality while industrial control systems and computing and network services associated with the bulk electric system operation. Although the critical infrastructure in reliability standards is not specifically mentioned in supply chain, it is important to emphasize for the

Commission that these standards adequately address the risks and creates a strong incentive for responsible entities working with suppliers and entities. A reliability standard of modifications of existing standards is not appropriate in the limited ability environment. For example, the NIST SV961 definition of supply chain is the integrated set of components, processes within the organizational boundaries that composes environment-enriching systems developed and manufactured, tested, deployed, and maintained when required with the Commission. Notice that this definition scopes activities go within the organization.

Life cycle of the industrial control system, which includes research, development, design, manufacturing, acquisition, delivery, information, operations, retirement, and disposal, is not entirely within the organizational boundary of electric power utilities that own and operate that system. The utility, environment, or boundary should be at the disposal.

Requiring utilities to manage risk in a research development, design, and manufacturing transfer risk known by suppliers to the responsible entity. These are in supplier environments, accompany the manufacturer control systems, and not within the utility environment. Also, utilities' influence and acquisition delivery and disposal

may be limited as third parties also play a role in these stages. Utilities can influence the acquisition in the building stages of contract negotiation through their suppliers, however this influence is limited. For example, mandatory requirements should be considered modestly of a supplier security perimeter, a utility would contact the equipment manufacturer and distributor to inform the supplier the need for physical security. The concept of enforced order is renegotiated to add additional items. To inquire security monitoring, the supplier issues an annual letter stating the compliance to the contract, and then the utility would perform a periodic presentation of the inspection. If this part of monitoring systems fails, then utility files a self-reporting non-compliance and possibly receives an enforcement action with supplier's management. This is adding a great deal of corporate-initiated administrative costs to service for the utility compliance risk, transferring the managing risk to utility, and not significantly improving the security posture of the utility. Therefore, any requirements to require the utilities environment organizational boundary, the utility's ability to control the risk and the owner's ability to comply may not be met. This is difficult in the acquisitional stages and any improvements to reliability is likely to be minimum, especially when you look at the

existing requirements of CIP Version 5.

In order to actually improve reliability, mandatory requirement must be achievable. If a mandatory requirement is aspirational, that is the required processes may not ever be developed, then utility can be burdened with documents with no improvement to reliability; we've experienced this under the framework. CIP Version 5 which introduced many new maturity requirements to the new systems under the scope of these requirements, always provides very strong supply chain control. For example, CIP 10, cyber asset chain management, requires responsible entities to conduct testing, vulnerability assessments required to connecting their advantage systems to the operational environments. And CIP requires sanitizing or destroying the information. These and other requirements contained within CIP Version 5 not only improve reliability of the bulk electric system but create stronger entities so they can incorporate cyber security requirements into their procurement process. It appears to me how regulatory procurement processes would improve reliability, the only improvements already addressed by the CIP Version 5 requirement. Instead I only see challenges because of regulations. For example, new requirements of existing spare equipment and utilities and supply chain inventory. Additionally, requirements may reduce the number of

suppliers. 800.161 recognizes and states: "An organization to assist community creates greater levels of transparency from suppliers must consider possible cost implications of such requirements. Suppliers may elect not to participate to avoid increased possibility of increased risk to the intellectual property, limiting an organization's supply to technology choices. The risk to suppliers is in multiple instances in different sets of requirements that may have to individually comply with which may not be scalable."

In conclusion, instead of creating new mandatory requirements, I strongly recommend that the Commission allow time, time to experience for these activities is needed to determine if there are any true reliability gaps that requires any requirements. Thank you and I look forward to further discussion.

MR. BARDEE: Thank you, Jonathan.

Next we have Nick Weber from the Western Electricity Coordinating Counsel.

MR. WEBER: Thank you.

Good afternoon. My name is Nick Weber. I serve as an auditor on the Western Electricity Coordinating Council cyber security team. I appreciate the opportunity to discuss supply chain concerns related to the bulk power system.

The goal of my remarks is to provide an overview of current increasing supply chain procurement initiatives, as well as opportunities to build on that work. Understanding the complex web of suppliers necessary to create new components is critical to the reliability of bulk power systems is no easy task. Nevertheless, continued efforts to understand and reduce threat is a necessary endeavor.

Procurement in supply chain security is not a new concept; the U.S. Department of Defense has been working on this for the past decade. Through my own short tenure at the U.S. Department of Homeland Security I was a part of no less than three separate inner-agency initiatives to address supply chain security and resilience. It is imperative that attributes of previous work be recognized and incorporated within any future standards or guidance in the agency.

I'd like to draw attention to four sec body of the work, as well as an anecdotal example of supply chain securities. This special publication 800.161 identifies the following three types of information: Communication, technologies, supply chain vulnerability. The systems or components within the system development life cycle is development and operational diamond directly impacting the life cycle, and the logistics group of transport delivery

systems and components. This 800.161 provides guidance to federal agencies identifying, assessing, and mitigating information, communication, technologies, supply chain risks, at all levels of the organization.

The scope of NIST 800.161 is germane to this discussion because the target audience and devices revolve around the federal ICT, not energy delivery systems. Critical infrastructure owners and operators can reference this in developing their own supply chain risk management practices. The American National Standards Institute, or ANSI, is partnered with Avid International developed as is SCRM 1-2014 supply chain risk management compilation of best practices. SCRM 1-2014 provides best practices from understanding the supply chain entities through protection and incident response to steady-state management and supply chain incident response. ISO 2800-2007 provides voluntary tests for the supply chain security. While the ISO standards provide excellent steps in security supply chain, they do not reflect the restraints of cost, nor the ability to review the operating governing body nor the consumer-enforced standards.

Balancing standards and requirements and costs is not a new concept depending on reliability standards, particularly the CIP standards, but it is a concern that must be continually addressed. These costs will come both

in the form of increased overhead to meet the supply's burden and increased prices for vendors who are unlikely to allow external requirements to impact their margins. As an auditor, I'm concerned with the ability to effectively oversee and audit the supply chain security standards since the target of the greatest impact is beyond my reach. This is where understanding of best practices and existing standards should be leveraged to identify where the procuring entity can have the greatest impact on securing their supply chain. Some of those areas might include supply chain managing, public/private information sharing, and procurement language. Effective supply chain mapping information sharing between owners and operators and the intelligence community can yield a significant increase in the purchasing entity's awareness and ability to understand risks brought on by specific risks in the supply chain. The single best example as to this is collaboration during my time at DHS. One of our class-led briefs an owner operator and an analyst asked audience members to come see him after his presentation on the system. It turned out a number of those devices had been compromised during the development phase.

The Edison Sector Control System Working Group, or ESCSWG, had cyber procurement language for energy delivery systems through a public/private partnership with

the U.S. Department of Energy and other government agencies in April of 2015. This document provides a strong starting place for any discussion in future standards. This document provides ample procurement language for energy leverage when drafting a request for proposal, given the limited capability of FERC, NERC, and the regional entities, to provide oversight of vendors and by extension their supply chains. Any future reliability standards should focus on the procurement of cyber actives critical reliability bulk power system.

Understanding and mitigating supply chain risk is a very complex and time-consuming process that will require a high level of collaboration between bulk power system entities, cyber assets, and other entities. I'd like to thank the Commission and Commission staff for providing me the opportunity to share my perspective and look forward to meaningful dialogue as a member of this panel.

MR. BARDEE: Thank you, Nick.

Next we have Dr. Art Conklin from the University of Houston.

DR. CONKLIN: I need to open my remarks by first thanking the Commission and staff for the invitation and opportunity to present to you. But most importantly, the views and opinions expressed here are my own and do not

necessarily represent the views or opinions of the University of Houston or the State of Texas, because I am a state government employee; so this is me, not them.

So who's me? I'm a hacker; I have two doctorates, one in EE, one in business. I'm in my late 50s. I now teach students how to break things, how to defend things, and I spend my evenings researching cyber security and critical infrastructure. And on the basis as I want to say as an engineer the power grid is an amazingly reliable instrument; you can't beat it. It finally surpassed even the phone companies on reliability on always being up. It all has changed, though. I'm no longer worried just about the laws of physics; I now have this problem of individuals hacking into things. And this set of risks we've been dealing with through a series of regulation and all sorts of industries; you've heard numerous comments on that.

NERC CIP is the path that we've used in the electric industry and it's been through numerous revisions to try to fix itself, to try to change, to try to keep up. I see the supply chain addition is just yet another opportunity to either go down the path of prescriptive guidance -- which I think we heard from previous people doesn't work -- or do we go down the slightly different path? And when I look at the different path -- I'm going

to paraphrase off my remarks because I like his short and sweet -- do we need regulation in this space? Yes, we do. The reason I'm going to say yes, we need regulation is, even though I'm anti-regulation personally, when you hear people discuss the argument of compliance versus security and yet both are in their inherit interest as a business to continue to have both, if they're debating between them then there has to be some upper hand that takes care of this.

So what would it look like? In supply chain we have to find something that (1) has to be mandatory or it doesn't exist. (2) But it has to be flexible. What I haven't heard anybody say yet, and I think is missing, is it has to be outcome-based. What are you attempting to achieve with your supply chain management? If you're trying to manage whether a vendor has a new product or not, then you have what we call the Juniper problem. Juniper Networks just recently had a very high-profile oops, bad code, in their code. They didn't put it in there, somebody else did. Who did that? It's not relevant to the discussion. But what is relevant is did Juniper fix it? Yes, they acted responsibly as a supplier. However, did the people who buy this material responsibly take their patch? If we made supply chain regulations, including like our current NERC CIP -- and there are some CIP regulations

right now that even if you wanted to apply the Juniper patch, you can't -- you will have to wait until it goes through this testing and all these other things and gets approved or an auditor comes in and say, "Yeah, you really needed to do that because that was really bad, it's not in the rules."

So we have to build something that's outcome-based on the outcome we wish to achieve. And it's not just I have to have an objective, "Oh, we have to have regulation", but what are we trying to achieve with the supply chain regulation? The risk in cyber can be direct, directly through our cyber system, or indirect through our supply the chain. Either one, we can't diversify that risk. And so here I want to say hats off to the person earlier from NIST; they did it. Even if the Department of Defense were to make all their systems through NIST's system, based on the NIST standards. They may tweak them right and left in their individual circumstances, but that's what they're built upon. Because at the end of the day it's built around trust. Does the Department of Defense trust their commanders to put the best systems on the field? Not really, they use regulations. Do we as a nation trust companies to do things? No, we have elected governments and we want them to regulate things. So there is a need for rules and regulations to resolve this.

The question becomes: What do you want to regulate? When you're trying to define for a firm to do what you think they should do, you have to define what it is you think they should do. And when you get into the specifics of a password should/must be so long, a supply chain must have 14 forms, things like that, then how do you respond to the following problem? "Oh, yeah, that didn't work. We're compliant, I'm here, we're compliant." "We're compliant" can't be a defense. In a supply chain, if I buy a piece of software and it doesn't work out with me, I have to have a backup plan, I have to have an alternative, that has to be part of, as Marcus put earlier, the business process, I have to have a business process and focus that will have that, that is auditable, that is checkable, if you go through all of the regulations the first speaker talked about they're detailed through all of those, these sorts of things.

So, I want to close by saying, yes, we need the regulations. We don't need something brand-new, we need to adopt what we know is working elsewhere, and we need to stay away from prescriptive, make it flexible, we have people go over the results. And "I am compliant" is not a defense. I look forward to questions and any meaningful opportunity to discuss with anyone. Thank you.

MR. BARDEE: Thank you, Doctor.

Our next speaker is Edna Conway from Cisco.

MS. CONWAY: Thank you. I'm just really honored to be here today, and on a personal level I have to say I'm pretty humbled to be in the experience and expertise that sits in this room today. So thank you for the privilege.

I serve as Cisco's chief security officer for its global value chain. Let me tell you what that really means: It means that we are embracing the higher third-party ecosystem that touches in any way our products and solutions. And that could be a service; it could be a component; it could be hardware; it could be software. So it is a very broad spectrum and I certainly have a deep appreciation for the complexity of a large-scale, international value chain. That's the background. And what I really wanted to talk to you a little bit about is a couple of things that were in my written statement. But first let me note that I'm tickled to be sitting next to Dr. Conklin because I am hoping that all of his students actually go work for my suppliers as white hats and if they go and work as black hats I will be standing there to fight them off.

We're really acutely aware of the convergence of OT and IT, and I think there's an important point. We've heard a lot about "do something that is similar to what others are doing." That convergence and the ramifications

of what I certainly worry about at Cisco, which is counterfeit, taint, misuse of intellectual property, and information security across that third-party ecosystem, is not necessarily a threat or a risk that is unique to the electric industry. I think you're heard today that it is actually quite common across, certainly for us, all of our customers that are governmental or not. The challenge I think we will have -- and we've certainly heard, I heard Mr. Sachs say, a great point, right, which is do something that makes sense for the industry but align it with others -- quite frankly, as a multinational, there are geopolitical events and positions that render it impossible for the entire world to come together. It would be lovely if it could; international standards are most important in that area. We've also dealt with the reality of a dispersion, a proliferation, of regulations and standards in the United State Government. So if you can get the Department of Energy to talk to the various groups inside of the DOD and talk to others inside of the U.S. Government, that would serve us very well and lead by example there.

First, what I want to say is what we really need do is understand the goal; I echo Dr. Conklin's point. And for us the goal is one that is interesting, and I know Mr. Boyens is here from NIST. And he and I have debated for

many years the chicken-and-egg problem of: Is security part of resilience or is resilience part of security? This is a unique approach, I think it's the right approach. Security is the senior most level and we believe it includes resiliency, data protection, trustworthiness, and privacy. So with that said, I think the next step for FERC should really be clearly articulating the threats to the goal of comprehensive security in light of that definitional parameters. This should include often-overlapping prevention, detection, and mitigation efforts. There's a reason for them to overlap, checks and balances make sense, our government is built on it.

At the core of that I think we need to say the perspective that we bring to the table at Cisco. The lens to which we see supply chain security risks really allows for two different distinct foci. The first is a focus on information and communication technologies in cyber risk. The second is a focus on addressing the full end-to-end spectrum of that value chain and looking at it with the lens of security technology, physical security requirements, and operational security deployed throughout logical processes. Without that, you don't have a comprehensive view. We believe FERC would do well to continue as it has, to go over those factors and areas of every effort of articulated that focus broadly in mind as

it addresses this challenge that we're here to talk about today.

We also believe that the expansion of the NERC CIP to include a new standard on supply chain risk management is not the ultimate path. In fact, imposing a new standard on an industry standard or other entities that provide products or services to registered entities, you can't have both, we sell to them. If you impact them with a standard, no matter how flexible, and not a guideline, it will be imposed on us. And we have ample years of evidence of how improperly flow-down clauses work. Procurement is important. Contracts do not create security in resiliency; they shift legal threat. That's why after 22 years as a lawyer I'm actually in business now; I didn't want to shift risk, I wanted to address security.

Let me highlight a couple of foundational elements I think the guidelines ought to approach. Approach taking control of retaining the particular member of the supply chain's flexibility to deploy the right security in the right node of that chain in the right time and manner. Deploying the right security in the right node at the right time, as you've heard here from many of us, needs to be undertaken in a risk-based manner. No enterprise, commercial, or government fully eliminate supply chain risk, that is a reality, if they intend to

remain economically viable and feasible. Embracing that reality will make success no longer achievable. Avoiding the pitfall of proliferation of new, albeit well-intended standard, or accreditation or guidelines is absolutely essential. Rather, a swift or, perhaps one might argue, more integrated choice would leverage the standards already in place, those include so many that have been articulated by my brethren. I will add one more, which would truly mean that the DOD uses to ensure that its ICT equipment that the wolf rider is using, which leads to ramification and death, is tested, and that is the ISO standard that -- the number is actually 1548, we call it Conroy material -- deep dives on security.

Bulk providers and distributors on this special set of procurement guidelines that are addressing the unique nature of their industry concern all of us as well, confidentially weighing the existence and robustness of a supplier's supply chain programs and procurement decisions absolutely essential, it can move the need up a lot faster than delayed contract negotiations and prescriptive standards. And in fact, it can encourage the individual elimination that each of the members of the supply chain bring to the table, which is actually why we included them in our supply chain to begin with.

I've also offered in my written statements and

it also appears in a NIST case study that we were privileged to be part of and highlighted on the NIST website the key domains for what I think might be more flexible architecture guideline. The most really include the identifying core domains within the architecture and it needs to embrace the physical, the operational, and the logical in addition to the cyber. And I've listed 11 domains in my written materials; I won't belabor the point by reading them out loud. But articulating around those 11 domains might allow NERC and FERC to come together and think: What do we have today? What have we heard? Can we leverage an architecture with really flexible methods of verifying the supply chain members' deployment of those kinds of guidelines and then use the same industry taxonomy of architecture and procurement-based validation methods, and that should take us to a place where no longer are we talking about just compliance or contract-shifting risk, but moving the needle together.

I'll leave you with this request: It would be Cisco's and my personal privilege to participate in any task force. We come at this because we understand we cannot do it alone, we must do it together, and we're committing to doing that. Thank you for the privilege.

MR. BARDEE: Thank you. And I would just note as someone, who myself practiced law for about 20-something

years, when faced with issues like this I wonder if I made such a wise choice in moving to this job.

But let's go to our next speaker, who is Bryan Owen from OSIsoft.

MR. OWEN: Good afternoon. Certainty of energy deliveries ties prosperity in practically every walk. Addressing threats to reliable energy delivery is well-deserving of a collective approach, and the Commission is to be applauded for respecting these accomplishments. I'm happy to be here today with me esteemed colleagues to discuss the matters important to managing supply chain risk.

So who I am? The principal cyber and security manager at OSIsoft. We're family-owned and -operated software company headquartered in Santa Ana, California. From to supply the chain perspective, we offer our products and rely on commercially off-the-shelf solutions in technology infrastructure. OSIsoft is also a global supplier, we have offices around the world. We are a presidential E award recipient for exports by the U.S. Department of Commerce.

Personally, my plan as a professional engineer is to apply my knowledge and skills to the betterment of human welfare above all other considerations. The remarks I express today are based on over 10 years of active

engagement in the industrial cyber security community, 15 years' experience with industrial control systems, and 20 years at OSIsoft serving our customers, many of which are responsible for reliable delivery of electricity in North America, and many others operating in major electrical loads. I appreciate this opportunity to contribute observations and views on management of supply chain risk, especially for software.

So the scope of standards to manage ICS supply chain risks, I believe the supply chain as many have said is very complex, globally distributed, and interconnected. Utilization is pervasive with hardware, software, computing and network services provided throughout the national infrastructure and in private enterprises. There are direct and indirect obligations imposed on suppliers and vendors that have significant potential for unintended consequence and market disruption. In that, ICT technology and ICS systems are so deeply entrenched in the bulk electric systems, inclusive of upstream suppliers, downstream loads, and may be necessary to approach the standard as a shared responsibility load. For example, fit-for-use in context of industrial safety hazards has been addressed using the shared responsibility. Standards are defined for safety and integrity levels and suppliers develop products for the most relevant use of these

products. Standards bodies are currently working to define security assurance levels that can be used to develop new products for ICS components with fit-for-use customers. Until such time ICS components build in security reliability, fit for use with high impact bulk electric system cyber systems, the scope of a newer modified CIP standard manage supply chain risk should be kept at a minimum and voluntary. Imposing mandatory supply chain risk management beyond the most essential controls where a foundation or legacy of ICS factors would likely exist only as a security theory. It should remain a high priority to enable rather than impose ICS, IT resources in the delivery of fit-for-use solutions.

Computing and network services further highlight the necessity approaching standards in the supply chain security as a shared responsibility. Existing CIP standards are unable to keep pace with direct innovation and computing and network services that is occurring compliance-audit approaches are not technically feasible for providers of moderate computing services. Thus, compliance implementation is a regressive force with respect to best-available technology through reliability and security. For instance, I frequently observe entities struggling to manage hundreds, and even thousands, of point-point VPN connection with external entities.

Whereas, computing a network provider's offered alternatives with innovative reliability and security features, such solutions are often dismissed out of hand due to compliance risk. A shared responsibility model for supply chain security should be developed, the scope of a new CIP reliability standard should be voluntary and minimal at this time. Development of fit-for-use specifications are proposed and is the basis for shared responsibility model addressing supply chain risk.

So what can we do? What's essential for standards to manage ICS supply chain managements? Essential should focus on the identity of software publishers and the associated response procedures. As a credit to the current CIP 004 reliability standards addressing personnel and training, in my experience these requirements already permeated throughout the ICS supply chain. Modifications of this standard would likely be disruptive and a diminishing risk reduction. However, identity of software publishers is a different story. The capability to identify software publishers represents a potential demarcation responsibility to defend important threads within the supply chain. Digital signatures offer a technical method that identify software publishers, as well as providing code authentication. Digital signatures could be a keystone for enabling ITS supply chain security

control through software, especially where control enforcement is already built into the underlying one-time platforms. The NIST 800.161 standard includes relating guidance and should ensure that code authentication mechanisms such as digital signatures are implemented to ensure software, firmware, and information of ITC supply chain infrastructure and information systems. And consider verifying integrity of software programs using, for example, cryptographic check, digital signatures, or hash code. Co-signing with digital signatures is widely accepted as good practice in the software profession. There are few implementation barriers related to code signing, although exceptions exist with scale and with technologies such as job security. Alternate mechanisms such as NIST national software reference library could be applied to identify ISC software and potentially its publisher. Commercial security services using binary techniques are also emerging fingerprint software enumerate to third-party libraries and the associated known vulnerabilities. At such time it is well advised for any newly-modified CIP standard to use the advancements of mechanisms used to identify ICS software publishers. Identity of the publishers within the ICS supply chain is important to incident response. Good practice like this are not necessarily notified about security issues

discovered in their software. This communication is bidirectional. Security issues tend to be silently fixed by the suppliers and vendors without disclosure to entities or industry coordination teams. Newer modified standards could improve communication and collaboration to related ancillary responses as needed. Under CIP 008-5 there is little, if any, incentive for reporting data to revise the implementation and violation threshold to award an offset credit to reporting incidents. Reports include such as discovery of vulnerability can generate a dramatic uptick of communication for security issues across the supply chain. Alternately a new modified CIP standard for improvement related to communication across the supply chain could be modeled after the voluntary aviation data reporting system.

In closing, changes in the threat environment signal the need for increased vigilance and due diligence throughout the ICT and FCA supply chains. The supply chain complexity merits the shared responsibility model based on standards developed as fit-for-use products and services. High-impact bulk electric systems should be the initial focus for fit-for-use standards. As an urgent priority, responsible entities need newer mechanisms to ensure the best systems operate the ITS software from their approved publishers. Incentives for reporting supply chain issues

should be addressed and newer modified CIP reliability standards as a catalyst for better communication and instant response capability. And finally the voluntary CIP standards for managing the supply chains should exclusively advance that available technology. Let's not let compliance get in the way of innovation.

Thank you for your time. I look forward to discussion.

MR. BARDEE: Thank you, Bryan.

Our next speaker is Alberto Ruocco from American Electric Power.

MR. RUOCCO: Good afternoon, members of the Committee. My name is Alberto Ruocco and I am the vice president and Chief Information Officer at American Electric Power. I am also the cochair of the EEICO Group and the AP Group. Just on a more formal basis, have in my previous lives spent quite a bit of time in manufacturing environments, understanding their supply chains, and my current responsibilities have cyber security team and the IT NERC compliance team at AP.

I really appreciate the opportunity to contribute to the discussion here. I will say that, given where I come in the sequence here, I'm going to modify my comments a little bit and not be too repetitive hopefully. I modified my written comments a little bit. For those of

you that don't know AP, we are one of the largest electric utilities in the United States. We generate -- well, first we support 5.3 million customers in 11 states. We are one of the largest generators of bulk electricity. We currently have 32,000 megawatts of capacity. We also own the largest transmission network with 40,000 miles of transmission and 220,000 miles of distribution wires. So one thing I would like to say is that, unlike some other participants in the panel, those of us that live in the utility world have to deal with this dual existence of living in a regulated environment and producing profits for our shareholders. So I will tell you that certainly provides a context for me that's important for you to understand.

So I think it's very important to state simply -- and I think it's been stated maybe a number of times in different ways -- nobody in this room or elsewhere can guarantee a risk-free supply chain period. No matter what we do, that will never happen in my opinion. So we certainly recognize the significant risk in our and everyone else's supply chain, and certainly with all the cyber security-related assets in our system. However, we recommend against a mandatory reliability standard for three reasons, and some of these have been touched upon before: First of all, FERC jurisdictional limitations I

think are our concern, I think Marc Sachs highlighted this well. And the fact that FERC really can't reach into the supplier network is a challenge. And it's unlikely, as some of the suppliers are represented here, that those suppliers are willing to share some of the information that we, as buyers, might be interested in or you, as a regulator, might be interested in for competitive reasons. I also believe, as many have stated, that the fact that today's world global supply the chain makes it fundamentally impractical to manage a standard with a grid network that has thousands and thousands of assets, each has a dynamic thing, multiple supply chains, and each is subject to ongoing potential design in the implementation changes. And third, we do believe, as many others have stated, that NERC CIP Version 5 provide adequate enforcements and management control for the bulk electric system; and I think Helen Nalley at Southern outlined that very well. So for these three reasons AP supports the voluntary development of guidelines through industry groups rather than a FERC-mandated reliability standard.

I'd just like to mention that if all of these previously-mentioned guidelines, principles, and best practices fail to identify malware -- so something gets through, all the way through the supply chain -- NERC CIP requirement 7, and in general cyber security best

practices, recommend the building of defenses and layers, or as was mentioned defense in depth. The current technology allows for continuous monitoring of all inbound and outbound and intracompany information communication. And if you have these tools in place, you will find and see anonymous communication. And those defenses in depth will protect. That's one way to think about it through the NERC CIP standard the effect that we have a backstop if you miss something in the supply chain.

I won't go over all the details of AP's cyber security programs and supply chain risk management program. Suffice it to say that the gentleman from BitSight did a good job outlining mature practices, and we follow those practices, and we continue to look for ways to improve; and frankly this entire experience has given me a number of ideas on how we can improve. I do think a particularly key point to make is that ultimately suppliers that prove to be the most reliable and secure are those that will emerge through competitive market forces. And these are the suppliers that will be available to electric utilities and other industries as well. So by way of example, just to extend on that point, as more companies and all industry adopt these supply chain risk managements programs, then more suppliers subjected to the scrutiny dictated by these assessment tools. Industry best practices will evolve and

will improve, and we at AP and others will benefit from continuous cyber security risk production. So fundamentally the market forces are going to continue to drive improvement in our vendor community, supplier community.

With that all said, AP will continue to collaborate voluntarily with other electric utilities, EEI, manufacturers, to determine best practices for enterprise supply chain risk management. Voluntary collaboration to define a uniform practice in the global industry and the suppliers will improve cyber security at a lower overall cost to customers then through a new incremental mandated risk management reliability standard. One example, for instance, is the Effery (phonetic) Organization. And perhaps we can, for example, leverage the Effery Organization to help test commonly-used assets and products. The shared lab resource will eliminate the need for each company to perform these testings and ultimately companies would more efficiently meet their cyber security risk management. So given the complexities of any one vendor supply chain -- and remember there are thousands for each of us -- and unique characteristics of each utility, I believe a reliability standard is likely to create inefficient and costly programs than they actually unnecessarily constrain a utility's supply chain cyber

security risk management program. In the end, each utility supplier base is different, so each utility would need flexibility to manage their supply chain risk in the manner best suited to their scale, scope, complexity, resources, and risk profile.

So I thank you again very much for the opportunity to speak and look forward to the questions.

MR. BARDEE: Thank you, Alberto.

And our final speaker on this panel is Doug Thomas from the Independent System Electric Operator.

MR. THOMAS: Good afternoon. First of all, I'd like to thank the Commission for allowing me to sit and discuss the issue of supply chain risk management. As previously mentioned, my name is Doug Thomas, I'm the VP for information technology and CI O for Independent System Electric Operator. So the views today are those of the ISO, they do not necessarily represent the positions of the association, nor the ISO RTO council, both of which the ISO is a member. So I think it is safe to say that regardless of our views, and our views on this issue are diverse, I think we would all agree that the Commission is faced with an important, complex, and difficult issue.

Determining the appropriate applicability scope for any standard of this nature is paramount and should be discussed with enforceability. Therefore any new standard

or requirement must apply to the same assets as those identified through the current CIP standards. Any new standard or requirement must focus on the same aspects of hardware and software, as well as people and services, irrespective of whether the best cyber asset is network, infrastructure, or solution-based. Furthermore and importantly, any standard should include services in the same manner as physical assets. In addition, any new standard should consider three interdependent but very interconnected categories of processes: Specifically procurement; design, build; and finally contract management.

So the question is why these three categories of processes? With respect to procurement, standards can ensure that the security needs of the asset owner are clear through vendor or vendors. With respect to design, build, implement, standards could require vendors to design products incorporating security from a variety of perspective. This would be done through the procurement process afforded by the contract management process. With respect to contract management, strong and robust contract management processes are key to supply chain risk management and they are the only means available and will need to address, not only the original purchase and delivery, but all aspects of ongoing maintenance. Finally,

standards should address the needs of periodic review contract performance, including compliance with contract requirements as they relate to security.

Probably the most difficult challenge is to understand or measure how effective security controls are within a vendor environment. This is where we need to look to the experience of other industries, such as the financial sector where they have spent many years developing and fine-tuning Sarbanes Oxley control which leveraged SSAE 16 audits or in Canada the equivalent SSAE 36.16 type lines. Controls will need to be risk-based and consistent with existing CIP standards, follow the traditional security model of confidentiality, integrity and availability. I recognize the development of a standard of this nature is complex and will require extensive stakeholders with many diverging entities. Although past experience indicates this process could take three to four years, I suggest that every effort be made to have the standards in place and enforceable within two years of the FERC order.

Finally, I would like to our Canadian, and particularly Ontario, aspect for consideration by the Commission. It is important to understand the national and provincial jurisdictions with respect to bulk electricity in Canada. Significantly, most of the relevant regulatory

framework is provincially based. As a result, the NERC reliability standards are applied differently in each of the provinces that have established agreements with NERC. Within Ontario, the ISO administers and enforces the reliability standard via the Market Assessment and Compliance Division of the ISO, which is a ring-fenced organization within the ISO. MACD manages compliance in Ontario in cooperation with NPCC. In Ontario there is no body that formally approves NERC standards; rather by default NERC reliability standards become enforceable in Ontario, coincidental with FERC approval. However, there is a provision for an Ontario entity to appeal to the Ontario Energy Board for a review of the standard, and the Ontario Energy Board has the authority to stop the standard from applying in the FERC doc to the standards of authority.

On the issue of Canadian contract law, contract law and tort law is similar in nature to the U.S. with a possible exception to jurisdiction. As in Canada the contract will specify a single jurisdiction for resolution of the legal issue. Other legal considerations that should be considered are copyright law, trademarks, competition, et cetera. Canadian case law in this area is still evolving and is not likely to present any barriers to supply chain standards but should be considered toward

standard development. At present, there are no specific Canadian regulations or standards that pertain directly to supply chain cyber security issues, and I am not aware of any movement in that regard.

I would make one final comment with respect to jurisdiction as a result of previous discussions. It is important to remember that NERC is the only regulatory body with jurisdiction in Canada, and the only organization that Canadian entities can provide formal input into during any additional drafting or amendments to standards or requirements. In closing, I would like to reiterate that the ISO supports and encourages the Commission with proceeding with the development and implementation of standards to address the risks associated with supply chain management.

Thank you very much. That concludes my prepared remarks.

MR. BARDEE: Thank you, Doug. And thanks to all of our speakers for their opening remarks; they've been very informative.

Let me turn to others at the table and see if there are questions from other people before I get to anything.

MR. PHILLIPS: Mr. Conklin, in preparing for the technical conference I reviewed a NERC industry advisory on

preventable investigative category 2B events and found three common themes: EMS software failures; adequate classing; and then problems with chain management. In your view do the current reliability standards require adequate testing levels for EMS equipment prior to deployment?

DR. CONKLIN: The answer to the question you ask, which was "in my view do they?" they can depending on how it's implemented. And at the end of the day it all becomes part of implementation, but I don't think the testing is going to alleviate what you cited as the problem either. Because a lot of the vulnerabilities and problems that will crop up in software and other things like this, they're not going to show up -- the ones we really worry about today, they're not going to show up until they decide to show up. And when they do, it's too late. So to answer that question: Do I think that the system as it's put in place today, if implemented correctly, could catch vulnerabilities? Some, yes; all, no. The critical ones probably not at all.

MR. PHILLIPS: Thank you.

MR. BARDEE: Anybody have anything?

MR. PHILLIPS: Actually, in thinking about this I kind of have separated the two into third-party risk and more supply chain risk, and I think sort of the proposal generally in the NERC order would address both. On the

issue of third-party risk, I had a few questions about just remote access and third party and how the current CIP controls address third-party remote access.

So, Mr. Kuberski, based on your understanding of how the controls apply, do you feel that this distinguishes between remote access from an entity perspective or a third-party perspective that are additional controls that a responsible entity must apply to a vendor third party? And then also do the standards permit vendors to maintain persistent connections?

MR. KUBERSKI: I think the standards do address third-party remote access; I don't see any eventual change events today. I will say this is one of my own beliefs: Your control system should not be connected to the Internet, and if they are connected to the Internet you really need to evaluate how that infrastructures are protected. So there's many layers of security in there to prevent anybody from accessing into the control systems. So to answer your question in short, yes, I do think the controls are there in place with the existing IT.

MR. PHILLIPS: Mr. Appelbaum?

MR. APPELBAUM: So, the third-party remote access tends to comply to remote access is what applies. It's clear you need to have a jump host to intermediate the system if that remote access does not occur from like PSP

that you control. So it's very clear. Now, when that person, if they're going to have control of the cyber system itself, then you need to have CIP 4 training, you need to be CIP 4 PRA. So it's there, remote access is already covered within the standard.

MR. PHILLIPS: Is there any sort of mandatory monitoring or control that you have over the vendor's access or have to do under the CIP standards?

MR. APPELBAUM: So, it's a trust environment. If they're remoting in, you already don't trust them, which means you're going to monitor their activities. If they have the ability to control and operate the system, now you're talking to them so you don't really need to monitor them. Both vendors and third-party entities cannot be trusted. At UIC we don't trust anybody for obvious reasons. So that's the answer.

DR. CONKLIN: I'd like to just bring up for remote access, un-trusted users is one thing. The same remote access allowed un-trusted users into Target. And the same remote access allows un-trusted users into our grid. And understand that CIP only applies to certain parts of our grid. But everything is eventually connected to everything. That's how malware gets to where malware wants to get. So I think it's very important to differentiate that we're not eliminating the risk just

because we agree that, "Hey, we're going to let X, Y, Z firm be a partner.

MR APPELBAUM: I just want to plug in, cyber asset controls that were just approved, they were there specifically for that. And I agree that that is a significant impact. USB sticks, vendor laptops being used to connect to our systems and do maintenance activity, CIP Version 5 can control those. They are there specifically to do that, you have to scan the laptop and verify the attack systems, verify malware engines. So, again, when we talk about supply chain and how CIP Version 5 works, a lot of things that go into that broad umbrella of supply chain risk, CIP Version 5 addresses a lot. And that's why we need to see how it's going to work out. I really think it does a very good job for what's within the organizational boundaries and not trusting anyone outside.

MR. OWEN: Just a supplier perspective: When all the same things that my colleagues talked about in terms of background checks and being sure that the CIP standards were being monitored, on our side of the link all came to me as well, all those sessions, all those recording sessions. I just wanted to emphasize that there are many indirect flow-through from these revelations.

MR. RUOCCO: Just to touch on the subject: Any of these I'll say attack of services are valid and worth

protecting. The one that I think is most critical and nefarious, I would say, is the hidden malware that's sitting built into the firmware, and I drop that piece of equipment into my network and I don't know about it. So I'm probably more concerned about that scenario than I am -- not that I'm not protecting against the other one, I'm just saying I'm more worried about the other one because it's just harder to identify.

MR. PHILLIPS: Ms. Conway, I think a lot of people have mentioned just sort of the potential impact having regulations come into one segment of the industry might have, and that might dissuade suppliers from wanting to participate. I guess my question to you is: Is the electric industry in the United States and Canada big in the matter if there were to be regulations?

MS. CONWAY: That's a great question. I would love to tell you that all of our customers matter.

(Laughter).

I think what we try to do, to be honest with you, I'm not sure that three years ago you would have found anyone with the CSO and supply chain, I think I was the first. Then we decided to put the supply chain and make a value chain and make it even bigger. And I think my answer to you is: If you understand the problem, you are going to be motivated to engage in your own enterprise risk

management for a variety of reasons. And that enterprise risk management plan has to address your supply chain third-party ecosystem. So the test really is not: Are you big enough? The question is: Are you a provider of a service or a product who is sufficiently cognizant of the world in which we live, that you are alert to the problems and what do we do about it? And if you're not alert to the problems then I'm not going to buy from you and I suggest that no one else should either.

MR. RUOCCO: I'll just add some color commentary because I deal with this, on not a daily, but certainly weekly, when it comes to procurement of equipment for IT and OT. The fact of the matter is, maybe notwithstanding the folks that are here in this room, but there are many, many suppliers that are fairly large that are still challenged to meet the standards and best practices that have been communicated. So that's the reality. But my point in my prepared comments is that I believe the market will drive them to compliance and in fact at some point probably exceed the practices of most entities on their own, if that makes sense.

MS. CONWAY: Can I just jump in for a minute? Because I absolutely agree with that. Let me just make something clear: I'm not saying you have to do everything with everybody; it has to be a risk-based approach. If I'm

looking at an ASIC supplier, to go back to your firmware issue. So you better understand the differentiation. Even the nature of the software, although the vast majority are problems are within the life cycle. So it's very interesting.

One thing I would guess, Mr. Phillips, is you confused me a bit, and I'm easily confused some days. But when you said the difference between supply chain and third party, from my perspective if you're in the supply chain you're automatically a third party. So there's my enterprise environment and everything else is a supply chain. There could be a supply chain that is my enterprise supply chain, so it's my own environment. And then there's the value chain. Are you thinking about it the same way, sir?

MR. PHILLIPS: Sure. I was just basically trying to distinguish, I think a lot of people are talking specifically about software and I wanted to make sure that we are also considering the third-party vendors they have access or performing the function for you that maybe don't necessarily build a product that is installed on the bulk electric system.

I have one more question, and I swear I'll be quiet. So during the development of the NOPR and the comments we received we had a few different suggestions,

some ranging the gambit from we could do a whole set of standards on this issue versus a few commenters said there are some things that we can do to sort of nibble around the edges of -- we can address things like watering-hole attacks, preventing or documenting practices. So I was just wondering: Is there some set of small things -- and I can put this out to the whole panel -- that we could do to the CIP standards to start to close some of this gap and bite down on the risk instead of a major initiative? Are there some smaller things we could do and look at and what would be providing that value for you in your opinion?

MR. APPELBAUM: As far as standards, I think in order what would I want to see if I was on the standard think tank team? And one thing that would concern me is that we would make a direct incentive that address supply chain. Because the thing is you need to know what risk and threat you're trying to address in the supply chain. "Supply chain" is just such a big term. Just as you said, third-party versus supply chain. It means so much. So we on the drafting team, we would want to know exactly what it is we are trying to address in that supply chain. And in my comments I talk about the seven stages of supply trying to point out there are stages we can't address. So I would hope you would say let's not go there, or if you want us to go there you'd be specific on it on what you want us to try

to write a requirement for.

I still think if you come out with "let's just nibble around the edges", my answer would be let's see what CIP version 5 does. What does it all address? There's a lot if you go down the list, boy, this is what has me concerned. I could come back and say this or this supply chain do not need a change, they're okay. There might be something that you're seeing that we could -- I think the Commissioner said something about common sense, making rules that make common sense into regulation. There might be something that could be done there. And you see the risk, the high-impact systems, again, trying to take that risk approach this already occurs.

MR. RUOCCO: So I just want to second the vote for this play-out NERC CIP Version 5. This standard has definitely been raised in particularly what I refer to as the OT world. We're in the midst of deploying these technologies. And I can see the impact that they have and will continue to have. So I think it's a good idea to play out CIP V 5 and see if there's a gap after that. Thanks.

DR. CONKLIN: Not to the contrary of the point of view already spoken. If you want to protect against watering-hole attacks, then -- you mentioned watering-hole attacks -- then you'll be attacked a different way, your problem will move. And so any kind of specific, once

you're going-after-business processes, this is going to be never-ending you'll never win this battle. So nibbling at the edges is just going to add paperwork and costs and trouble for all of the providers. So I'm going to say, yeah, you should let NERC CIP run its course, which you've heard. However, if you think that's going to solve your supply chain issues, you clearly live in Denver.

(Laughter).

The altitude's higher. The issue really is it's one of accountability and how do you issue a standard that says you need to identify supply chain issues. And I think we did a great job of summarizing that. And that's what we need to do. You need to understand: What are my risks? My risks are different from an ASIC, from a cable, my risks are different from on software depending on where I'm putting it in, what it's doing, where it came from, and what libraries are included. And when I pass those risks onto my customers, how do I communicate that to them? How do I work with them? And so there has to be some method of telling all the parties concerned you have to do the right thing and if you don't do the right thing, I'm going to pull you over.

I got pulled over once for speeding in Wyoming, and actually I didn't get a ticket for speeding. He said, "You know, you disrespected our local custom", and they

actually have a law in the book for disrespecting local customs. And I thought that was kind of interesting, it was really in retaliation to a regulation that said if you pull somebody over for speeding the state gets the money. If you pull somebody over for other laws the county gets the money. And so they made a rule that said disrespecting local custom, which covered all sorts of other laws, and then they got to keep their money. Be wary of whatever you invoke, they will find a way around to achieve their goals as opposed to the outcomes that you wanted.

MR. APPELBAUM: I have something to say. Your question is very, very important. Your supply chain risk is always going to move, right. There's always going to be that risk. You can't say there is no bad guy out there. That's why I think this panel before you and the next panel keeps going back to 10, this requirement. Connecting the cyber system at a high level we check those controls. And that's because nothing that comes before in that supply chain, bring that device in, can one hundred percent make it compliant -- make it secure, not "compliant". I made a mistake myself. Make it secure. They're only protected before you put that EMS system in or that high-impact relay, you need to test it, you need to go through it. Is my password there? Do I have that right baseline? The baseline I put on there, is that the baseline I expect to

be on that system? These are all checks in existing lists and various documents. But that's what that CIP 10 or 5 is supposed to do; it's a very important step, chain management step, it's key, and there's a lot that goes into the work, the reliability assessment.

MR. OWEN: I'd like to encourage to not be too quick to dismiss the idea of low-hanging fruit. And the notion of like Havix (phonetic) had last year was software that wasn't signed at all really as a supplier to this industry is embarrassing to me. I think that regulation is not required a voluntary approach that simply makes it clear that that's the expected normal in this industry and shaming your peers when they don't do the right thing would be sufficient.

MR. THOMAS: I think I might say with respect to whether this view there should be new standards that should be developed now or whether or not there is a view that we should let CIP V 5 settle for awhile. To ensure that you're nibbling around the edges in the right area you really first of all ought to undertake a more holistic review. Now after you undertake that more holistic view, you may then decide to focus on certain areas. But I would encourage some sort of overall holistic review before starting to target specific areas of procedures which will differ in terms of both importance to corporations and

their willingness to address them.

MS. CONWAY: All right, so one last thing: This is a model. What we did is we looked at what was out there. I started with over 3,000 controls and I narrowed it down to 1,200, and then I got serious. And in our architecture there are 184 requirements. That's it, 184 across 11 domains, and not all of them apply to everyone in the matter of the nature of the service of the product that you're offering as a member of that value chain. So my answer to you is: There is a way to narrow it down and articulate a baseline. Many of those things are already articulated, but that kind of comprehensive view might assist us in identifying what's out there. And to Bryan's point, if there's low-hanging fruit that hasn't been addressed, let's close the gap.

MR. PHILLIPS: Thank you all.

MR. WEBER: One more for just a possible nibble there. I think it's important to understand who's manufacturing the subcomponents and where they're being manufactured, and then also maintain a global situational awareness. You've seen the presence of that in CIP 14 requiring entities to plug into the vectors to understand how they can be compromised through the attack chain. I think that's something that can be done.

MR. BARDEE: Dr. Conklin, I have a question for

you just so I can try to understand a little better your written remarks and your statement here today about outcome-based approach or risk management framework. Using that in the context of a regulatory scheme such as we administer, how does that look, how does that sound, when you shift from, as you've described, the CIP framework to management framework?

DR. CONKLIN: Again, preferencing just how much I hate regulation. But Sarbanes Oxley, we had a lot of problems with financial controls in our various companies and we tried various SET rules and all sorts of entities said thou shall not cheat on your books. We got very specific about how would do appreciation, all these different swaps, everything in the world. At the end of the day the regulation that really matters is the regulation that says those that sign, which would be CFO's, CEO's, and some cases CIO's for very specific purposes, if it goes wrong, it's on you. And includes criminal provisions. So if you lie or you misrepresent or you basically sign stuff that shouldn't ever be signed because it's not true and you should have known better, whether you did or didn't, you can go to jail. It suddenly got a lot harder to get things past a CEO when they did that. So there's an outcome of if things go wrong, why did they go wrong? What controls did you have in place? Without being

specific about them. Sarbanes Oxley does not list, "Well, I did this, this, and this, therefore you cannot jail me."

So things will always go wrong, you can't regulate about things going wrong. But you can regulate against: Did you take due diligence ahead of time? And that term is pretty well understood by lawyers. And if you didn't, then you suffer the consequences. Now, it's very difficult, the one difference is Sarbanes Oxley, you really can't fine someone along the way. You can't say this is a little off and this should be more forward here, therefore here's your penalty clause. It's really almost like a death sentence only. But it really has had a dramatic effect on keeping people focused on not -- don't let things go wrong, but understand you're in charge of this and you're responsible for this and if you don't do what you're supposed to be doing we'll get somebody else to do it. And that's the other aspect. In this industry how many people in positions of power that should have done a better job have been barred from working in the industry? If you go look at business under Sarbanes Oxley and other things -- with the exception of banking, we won't go there -- there have been some really profound people at least from other companies and part of the SEC they can no longer ever be on a board of directors or ever be in charge of any company ever again. So that's sort of accountability back towards

some of these things, is how you're going to have to do on at outcome base. That's something I wanted to make sure you know. I don't want companies to keep making mistakes. That's the sort of the direction I would look at the way.

MR. RUOCCO: If I can comment on that as someone who has to sign those documents.

(Laughter)

Hopefully, you won't see me on the news tomorrow. Take the scenario of a zero day. I could be the best CIO, CSO in the world and a zero day comes through that just was a clever way to get in. And had I done my due diligence, had I done the proper preparations, et cetera, taking proper precautions? So I do think it falls apart a little bit in that scenario. Otherwise, I understand your point. And I certainly pay attention to those things that I have to put my signature on. But I do think the scenario in the zero day makes it a little bit tough to hold that standard.

DR. CONKLIN: If I can answer real quickly. I wouldn't say zero day -- let's take something that's not a zero day, black energy. Does black energy exist anywhere in your systems? You can't answer because I don't want you to be on the hook for that. But the answer is definitely clearly, yes; it's all over our grid. I know I've gone and seen it in various places; it's all over. That in its own

right isn't necessarily the issue. The issue is: Will it take down your grid? Have you structured and done the things necessary so that should a bad -- a tree branch fall on the wrong computer, the wrong substations, at the wrong time, yes, you're going to have some outages, those things all happen. But do you have the right things in place to recover appropriately to deal with all those things, including zero days. So I'm not anti things going wrong. Things are going to go wrong. Black energy is out there; it's going to be all over our grid, you're not going to stop it. However, can we stop it from taking down our grid, that's the answer. Are we going to get products from third parties, i.e., other countries, other companies? I don't think country is really an issue because bad stuff is made here in the U.S. as well as anywhere else, that's not the issue. Are we going to get bad stuff in our supply chain? The answer is yes. Do we have a method of dealing with it when it doesn't work out?

I rented a rental car in Hawaii recently, Nissan Ultima. I will tell you don't rent those when you're in Hawaii because they have a little digital keying problem and every so often it says "incorrect key ID". When you're in the middle of nowhere and the key is not working, it's a bad day, okay. And there's no backup plan at that point. I now have a new backup plan: I actually ask at the rental

counter, "If this sort of thing happens will you come get me?" Okay. So I think knowing what to do when things go on is what we have to hold people accountable for, not the going wrong.

MS. CONWAY: May I comment on one thing at the risk of stating the obvious. It's pretty clear that ITS putting together a task force is -- in addition to wanting to go out for a drink with these folks on the panel I think would be fantastic conversation, it would only be a milkshake but it would still be a fantastic conversation. There are so many of us that are passionate about this and who understand we can't succeed if we do this together. If you get nothing else here, that so many of us are willing to -- this is our country, this is our grid, this is our industry, and we're in it together, we want to help.

MR. RUOCCO: Thank you. I'll take a milkshake, chocolate. A few people have said this, and I think this is something perhaps for you all to think about, is holding people accountable to response standard might be an interesting direction to go. I think many of us have the capability to identify a number of possible intrusions, in some cases maybe even address zero day scenarios. But I think the industry is aligning further, is prepared for that scenario if something gets through. And I'm not sure I have the answer, so maybe the task force can help us.

But I think the notion of things you ought to respond to and a response plan given of a particular scenario or some event is worth thinking about. Does that make sense?

MR BARDEE: Well, thanks to all of you. We really appreciate your attendance and efforts today and your insights. And thanks again.

We'll be back in 15 minutes at 3:35.

(Whereupon, a short recess is taken.)

MR. BARDEE: We're back for our third and final panel for today. We're all in place. With that, I will turn it over to Douglas Bauder from the Southern California Edison Company.

MR. BAUDER: Good afternoon. Thank you to the staff for allowing me to take a few moments to talk about how Southern California Edison addresses supply chain risk management. And what I'm going to say has been said here before. I think you'll note my resume is a little bit different: I've spent about 20 years in the power industry not only as an electric operator operating control systems, it could go the wrong way if there was a latent problem, but also overseeing physical security and also overseeing cyber security under the NRC rules. So I have some perspective on risk versus award in that area. I'm chief of procurement officer and vice-president of operational services at Edison. I also oversee security business,

resiliency, real estate, and a number of other functions at the company.

I am very familiar with what we're talking about here today in terms of risk. And I'll tell you that cyber security is an issue of paramount concern to us at Edison. We've devoted several thousand resources to protect the grid from cyber attack. We know that the region we're in is particularly sensitive, so we pay attention to that. We do share a common goal to enhance the safe and reliable operation of our grid. However, as I will discuss today, Edison believes to develop new regulatory requirements and standards focused on supply chain issues simply would not assist in achieving that goal in many ways, and I'll share some of those ways in a little bit. But we do share the Joint Trade Association's view that there's no regulatory gap to be filled regarding supply chain cyber security. That issue has been amply discussed in the comments filed by the trade association, by the NOPR dated September 21st, 2015.

With that said, we do acknowledge that the Commission has expressed sound concerns about the supply chain cyber security risk that should be addressed. Also, we believe that the CIP V 5 framework, recently approved, was designed to address and mitigate the various, new-evolving threats. And we've talked some here today

about CIP 10 and how CIP 10 addresses change management. Specific to high-risk bulk electrical system changes, we talked about how latent changes are addressed, so I'm not going to get into much of that. But we believe that that framework is effective. We also believe that the existing standards, how they require entities such as Edison to develop prudent and effective vendor risk management processes are also affective. For example, CIP 11 includes information protection controls; CIP 4 includes vendor personnel risk assessment and access management controls. Thus, entities such as Edison are already required by existing standards to manage supply chain risk, including those risks introduced by third-party vendors. There's not a lack of security control over managing supply chain risk.

In addition, though, is the standard. Understanding and managing risks from our diverse supply chain is really an important part of our strategy. Southern California Edison expects each of its suppliers to deliver products and served that will not introduce threats to our environment and protect all SEE information that a supplier may have access to or generate in the course of doing business. We implement these expectations through a number of practices and protocols, including segmentation of our suppliers by a list of factors. We actually use an enterprise of risk management mechanisms to do that, and in

that mechanism we look at grid reliability and factor it down to: What are the suppliers in that space? We implement the comprehensive supplier qualification program and on-boarding process, in addition to the background checks that are required by CIP 4. So, for example, we look at a supplier's financial, we look at a supplier's history, we look at what they've done before our company and scorecard that work. We look at what the supplier is going to be involved in: Is he going to be involved in grid assets? Or touching personnel information at out company? Or what that particular work is.

Then we use cross-functional teams to evaluate and do that vendor risk assessment and various procurement efforts, grid-related or otherwise. The teams particularly involve supply chain management, information technology, our transmission and distribution team, our legal team, enterprise risk management which I just mentioned, and other stakeholder personnel. And also importantly including the cyber security procurement language into our contracts.

We've talked about contracts a little bit here today, and are they effective? Well, I'll tell you that requiring cyber insurance, requiring third-party audit rights to make sure that the cyber programs that a vendor is using, requiring financials in particular for a vendor

to be able to withstand situations that involve response to cyber issues, and requiring a vender to disclose to us other cyber issues that have occurred are important. The back end, yes, maybe the event already happened. But when we're in contract space with a vendor, they know how important these things are when we put them in a sector when we acquire these things. These are practices that we do based on the risks that we see and that risk is based on what those vendors are going to be touching on, what they're going to be working on in our system.

We also do regular contract operation, that means require score cards and performance metrics. So as we have a vendor at one of our facilities, an example would be a vendor under CIP 4 controls, if there's issues with that vendor we'll score card those issues and roll them up and the vendor may not get additional work with Edison the next time we go out to bid. These practices, along with the existing standards, provide utilities like us with flexibility to remain versatile and effective in meeting our supply chain landscape.

Next, we're concerned that the development of new regulations focused on supply chain management could have unintended consequences and end up hindering rather than helping entities protect the grid. That's been discussed here today as well as being prescriptive to a

standard, meeting the standard, but not necessarily be leading-edge in terms of teaming with a supplier to ensure we're implementing best practices. I've seen first hand the impacts of some of the most restrictive supply chain regulations in other fields, and fear that the adoption of such restrictions overall entities will not address the concerns the Commission raised in the NOPR, it could have worse secondary impacts on our sector. For example, in position of NERC regulatory commission-style regulations may drastically limit the basis of suppliers available to electric utilities and stifle innovation. That's not theoretical in nuclear power; I've watched under the NRC's NTFR 50 program, I watched vendors merge together so eventually where we had 12 vendors we now have one or two, and the costs escalated. A typical cost escalation we would see was 3 to 10 times cost.

Another big difference in the NRC's regulatory scheme under the 10 CFR 50 appendix bravo, the vendors needed to qualify in the program needed to have a quality assurance program that enables them to meet our requirements and meet the regulatory requirements. So if there's an issue, the Nuclear Regulatory Commission can go after the vendor and audit the vendor along with the responsible entity. I've seen that happen in nuclear power. The vendors know this so that they brace up their

controls, they do things like source documentation, a lot of witness documentation, a lot of traceability, and that raises the cost of all of the parts that we use in nuclear power, whether they're cyber or not as they touch the nuclear power plant. I've got examples of those if you'd like some specific examples, I won't name vendor names. But I will tell you that the cost impact can be huge. So what happens is some level of creativity is ruined; vendors consolidate; and costs go up. A few vendors take on the burden to meet the requirements. Many choose instead to forego the market of NRC customers, the procurement regulation model stifles and constrains further developments in the field due to increased costs during cyber security solutions. This means entities such as Southern California Edison could be forced to select protective equipment from a small pool of offerings rather than from a much larger pool. We know that in cyber security it's very important for those folks that are out in that leading edge to develop new methods to prevent and detect issues. The small size of available vendors in a very highly-regulated environment also impose operational cost burdens on to our entities and their ratepayers in fact. Those vendors that do adopt the regulatory burden increase their costs accordingly, covering the administrative control. And those costs would, if a

similar model be adopted to the CIP model, be passed on and turned to us and then turned to our customer.

With these two concerns in mind, Edison's respectful recommendation to the Commission in this proceeding is as follows: First, Commission should reconsider its proposal to adopt new regulations focused on solely supply chain management. The existing NERC CIP standards already address the generalized concerns expressed by the Commission. Further, development of new regulations and requirements may hinder rather than help us in the utility sector from pursuing additional risk, mitigation, and managements efforts, and technologies that could in fact protect the grid.

Next, we propose that the Commission encourage utilities to continue to identify and develop supply chain-related cyber security best practices where possible, but not necessarily manage. For example, as cited by the Commission in the NOPR, the National Institute of Standards and Technology, NIST, has published the supply chain risk practices could involve and provide entities, such as us and others, guidance for tailoring and implementing these practices. We've discussed the NIST SP 800-151 and NERC already. However, because one size does not fit all, entities must be free to use, modify, or not use these practices to fit their own requirements. Similarly, the

Department of Energy published a set of cyber security procurement language, that we've also discussed in here today, that provide a starting point for entities to use when acquiring energy delivery systems or components. This publication is voluntary and entities such as Edison are free to utilize the information provided by the DOE guidance to enhance their own systems.

We do recognize that cyber-related threats to the industry and its control systems are constantly evolving and we need to be evolving our capabilities to address those threats. We remain vigilant and committed to implementing heightened security measures, both physical and electronic, to ensure that reliability protection of the grid. As such, we continue to monitor the grid and take actions, as other utilities do, to address those risks introduces through the supply the chain. Thank you.

MR. BARDEE: Thank you, Douglas.

Our next speaker is Andrew Bochman from the Idaho National Lab.

MR. BOCHMAN: Thank you Commission, thank you staff. My name is Andrew Bochman from the Idaho National Lab where I'm senior cyber energy security strategist. I'm here on behalf of the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, DOEOE. And the DOE's complex is of 17 national laboratories, one of

which is the Idaho National lab I'm from. INO has a long history cyber security physical research, which is development of the world's first nuclear energy generation technologies. This work involved designing and testing nuclear generation plants, as well as the first conductor control systems, essential for monitoring and managing nuclear proxies at a safe distance. Over time this led to working in close collaboration with a variety of energy and communication suppliers as all parties sought to achieve maximum security goals.

In large part, based on these experiences, INO was approached by DOEOE to performed ICS assessments and impact demonstrations on a large number of systems involving many suppliers and asset owners. DOEOE has undertaken a number of initiatives in the sense of improved innovation stance, vis-a-vi energy sector supply chain vulnerabilities and related challenges, particularly to the electric, and oil, and natural gas sectors. Among these is the cyber security capability maturity model, abbreviated C2M2, which includes ten principle securities, one of which is supply chain and external dependencies management. It addresses cyber security requirements for electric utilities and other asset owners and their suppliers and third parties such as requiring suppliers to notify customers if and when they themselves have cyber security

incidents, or if they themselves uncover, otherwise learn, of vulnerability inducing product defects throughout the extended life cycle. Asset owners are also encouraged to monitor other information sources closely to identify and avoid supply chain threats. I'm sure you're very familiar with by now, DOEOE and many of the organizations have produced procurement language in 2014 to guide and assist folks in trying to add supply chain and other security factors into their supply chain to assist asset owners in their acquisition of more secure products and services.

One thing I definitely want to share with you is the formation of a new energy sector critical manufacturer working group. A collaboration effort between the DHS Office of Infrastructure Protection and DOEOE that will work with the energy in critical manufacturing sectors to evaluate the security and integrity of delivering devices, equipment, and services that support the nation energy infrastructure. This supply chain focused effort will provide a forum for asset owners and manufacturers to discuss critical issues that might impact the energy sector and provide recommendations for areas of improvement.

Here are a few early details for you: As currently envisioned -- here's another great acronym -- the EFCMWG, again that was Electricity Energy Sector Critical Manufacturing Working Group, will (1) Be composed of

members from the critical manufacturing sector coordination council and the electricity sector coordination council of the natural gas sector coordination council. (2) Provide an open dialogue in a CPAC environment where critical manufacturers and energy asset owners can discuss issues that impact the energy sector, be it critical manufacturers and the supply chain. And (3) bring in, as necessary, subject matter, supply chain management, trade organization, et cetera, to contribute their specific expertise on the issues being discussed. We briefed the consent for this working group at the Association of Electric Equipment Manufacturer's annual conference, that's NEMA, N-E-M-A, as well as the Electric Subsector Coordinating Council and the Oil and Natural Gas SEC meetings last November and December, and got very strong approval to proceed. If the ESCMWG is successful, one tangible result -- and I'm coming down the homestretch -- you main envision us as the next national grid security and resiliency exercise, grid X4, which will be in 2017. Not only will asset owners and government agency senior leaders be at the executive table top, but so will critical manufacturers, or in other words some of the most important energy sector suppliers, to help steer us towards the best possible responses when security and the grid and the nation are at stake.

Thanks again for the opportunity to share this update with you.

MR. BARDEE: Thank you, Andrew.

Our next speaker is David Whitehead from Schweitzer Engineering.

MR. WHITEHEAD: Good afternoon Commission members and the Commission member staff. I'm Dave Whitehead, I'm the vice president of research and development at SEL. I'd like to provide perspective of a supplier to our regulated entities. And before we rush off into the regulation, give perspective on really what the industry is doing from a supplier perspective on supply chain.

So, SEL partners with customers around the world to ensure the safe, reliable delivery of electric power needed to design manufacturing, supply a products and services and ranging from generator and transmission protection to distribution automation and control systems. We have been manufacturing our products here in the United States which were founded more than 30 years ago. Managing supply chain risk is a fundamental component to make sure that the quality of the products that is being delivered to critical infrastructure owners and operators.

At SEL we continually identify and measure our proven practices in order to exceed the reliability

expectations of our customers. Our supply chain today is global and complex, therefore SEL takes a comprehensive approach to evaluating the risk to our supply chain. Due to the rigorous design and qualifications process in the research and development division that I lead, SEL works to evaluate and understand all potential variables in supply chain risk. The following are just a few examples in the way we work to ensure a dependable supply chain: This week at SEL we hosted our 16th annual supplier conference. During this event, which encompassed more than 200 different companies, we explained to our suppliers how the reliable operation of power systems depends on the quality and reliability of SEL products. We shared our technical needs and strategic objectives for the coming years and identified ways to partner to make sure the continued supply of quality parts. Attendees include those that supply component parts, equipment, and services. This relationship-building continues throughout the year as we conduct onsite audit inspections of many of our suppliers to ensure that their quality security processes meet our required specifications.

At SEL we deploy supplier-rating relating systems that include intelligence across the company to assess risk variables such as manufacturing location, material lead times, financial health, replenishment

methodologies, technology type, and performance for on-time delivery. As much as possible, additionally we ask our suppliers to first identify their suppliers along with their mitigation strategy, strategies in replenishment methodologies to help us better understand their risk of their various suppliers.

As the Commission noted in the notice of public or purpose rulemaking, product integrity is essential to the protection of the bulk power system. In order to ensure the integrity of the products we deliver to our customer, SEL employees' qualification process for all components we purchase, we procure the components directly from manufacturers or official distributors. The component must be purchased on the site of processes we take additional steps to ensure their integrity. We develop the majority of our own software. If we do use third-party software, we require the source code. All products go through numerous code peer reviews. We also have automated tools for inspecting the code in order to identify potential issues developers may have missed. Further, we provide tools to our customers to ensure that they know that the software came from SEL.

We participate in various government-led initiatives and standards, developments, and activities so we can be cognizant of other current best practices,

attribute to the industry best practices, and stay attuned to the evolving demands based on our customers. Similarly, we contribute to and use guidance documents such as the NIST cyber security framework to improve our own processes and controls and help shape agreed-upon industry best practices.

I'd like to do close that SEL does not think a mandatory reliability standard would help registered entities mitigate the risk posed by their supply teams. Giving entities the flexibility they need to manage global supply chain grid is extremely important in this day and age. To do that effectively, we must be able to use any and all tools that are available and improve upon those tools through innovation. Various standards, such as the one that I mentioned earlier ISO 27.001, provide SEL with the tools we need to manage risk in the supply chain. In order to make electric power safer, more reliable, and more economical, we need to be able to move at the speed of business. By their very nature, standards are restrictive and often too slow to keep pace with the technological development. Being required to adhere to a standard does not always practically mitigate its risk. SEL's continued innovation, as SEL using the best parts of standards rather than simply settling into what may be required. It is in the best interest of our customer and their suppliers not

to limit the tools they have available to them to mitigate risk or the supply chain. To that end, we will continue to collaborate with our customers in their efforts to protect their critical infrastructure assets by helping them ensure a dependable and diverse supply chain.

Thank you again for the opportunity to discuss this important topic.

MR. BARDEE: Thanks, David.

Our next speaker is Andrew Ginter from Waterfall Security.

MR. GINTER: My thanks to the Commissioners, and to everyone, for the opportunity to address you today. Waterfall Security Solutions is a technology vendor producing a family of products based on security gateways.

The bulk electric system supply chain provides both physical and cyber products and services to NERC entities. Almost all major industrial vendors have cyber or cloud offerings which are used widely within the BES. Almost all of these cloud products and services have connections to acquire control systems and sometimes demand remote control all from vendor control centers via the Internet. Compromise of vendor cloud systems can provide an attacker with the means to attack hundreds or thousands of cites in a North American grid simultaneously. For example, many entities with large power plants have

stagnated their plant networks by deploying just a handful of firewalls. When CIP Version 5 takes effect, even the largest of these segmented power plants will have no high-impact BES systems and no medium-impact systems. This is because each network segment controls less than 1,500 megawatts of generator capacity. Now, don't get me wrong, segmentation is a legitimate security technique when the result is truly independent segments that make it impossible or difficult to propagate an attack from one segment to another and difficult or impossible to attack all of the segments simultaneously. However, connections to cloud systems, and even to corporate IT systems, pass right through firewalls.

At Waterfall we know this as the NERC CIP firewall loop hole. To address this threat, a growing number of forward-thinking entities deploy unit-directional security gateway technology to protect important networks, including segments, firewalls. The gateways physically prevent any message from a cloud vendor or an IT member from reaching a protected network. Cloud providers can monitor unit-directionally protected networks, but can neither control those networks nor compromise them. Entities can legitimately deploy security controls to unit-directional segmented networks because such networks are effectively immune from simultaneous attacks, as well

as many other attacks. If vendors need to make changes to protected systems, the unit-directional remote technology lets the vendors see the screens of BES control systems and provide advice to local personnel, making changes without risk to those control systems. This is in contrast with CIP compliant interactive remote access systems, which can be breached by attackers of even modest means. Security bypass technology is another option for unit-directionally-protected networks, entities activate this technology manually to provide a vendor with remote control of an otherwise unit-directionally-protected system.

The NERC CIP Version 5 standards encourage the use of unit-directional gateways by reducing compliance costs for unit-directional protection systems. CIP Version 5 exempts unit-directionally protected systems from bidirectional external connectivity requirements. In other jurisdictions such as Europe, the Middle East, and along the Pacific Rim, electric utilities are also using unit-directional protections including cyber supply chain risks. The same is true as other industries, including offshore platforms, petrol-chemical pipelines, and control systems.

The Department of Homeland Securities, NSIC, recommends unit-directional communications in seven

strategies, including the network segmentation strategy. To this date, 182 Revision 2 positions unit-directional gateways as stronger than firewalls in defense in-depth programs for industrial measures. The Commission may also wish to examine the cyber supply chain risk address by the French ANSSI, that's A-N-S-S-I, not the North American ANSI. The French standards for building firewall connections between the most important critical infrastructure networks and any less critical network, that that is for build remote control of the most critical networks. The French standards don't permit unit-directional monitoring of all networks and recommend unit-directional communications over firewalls.

When NERC entities, in our experience, ask industrial vendors for increased security in the form of unit-directional protections, we see an entire spectrum of responses. Some vendors embrace unit-directional technologies; others permit unit-directional gateways from continuous monitoring but demand security bypass technology for occasional remote control; still others reject unit-directional technology, outright arguing, in my opinion incorrectly, that firewalls and encryption provide sufficient security for such connections.

And if I may add to my prepared statement regarding the most-pressing practices, to focus on whether

regulated or not, yes, all security measures can be defeated. Our goal, though, should be to raise the bar, to raise the bar to the point where the only practical effective attack on our most important systems is one that requires deliberate, physical cooperation by people at the targeted cite.

To sum up, critical infrastructure sites in many industry's jurisdictions use unit-directional to address industrial cyber supply chain risks, and so work to raise the bar in this way. Increased use of unit-directional security gateways involve electric systems will dramatically reduce cyber supply chain risk and will measure the improved security and the reliability of the bulk electric system.

Thank you again.

MR. BARDEE: Thank you, Andrew.

Our next speaker is Steve Griffith who is with the National Electrical Manufacturers' Association.

MR. GRIFFITH: Good afternoon members of the Commission staff. Thank you for the opportunity to allow me to participate in this conference. My name is Steve Griffith and I'm an industry director representing the National Electrical Manufacturers' Association, NEMA. NEMA is the association of electrical and medical manufacturers founded in 1926 and headquartered in Arlington, Virginia.

Our nearly 400-member companies manufacture products including power transmission and distribution equipment, lighting systems, factory automation, and control systems, and medical diagnostic energy systems. NEMA and its member companies interface with several of the 16 critical infrastructure sectors, NEMA is one of them. NEMA understands that a focused effort as a number of companies is essential to support this critical infrastructure essential to nation security.

As the manufacturers of critical grid equipment, NEMA and NEMA companies play an important role in strengthening the cyber security in the electric supply chain. NEMA and its manufacturers understand that securing the supply chain is essential to securing the grid, and that cyber security aspects should be built into, not bolted on, manufacturer's products. We also understand that managing cyber security supply chain risk requires a collaborative effort and open lines of communication among electric utilities, companies, and the manufacturers of critical electric grid systems and components, both hardware and software. The Edison Electric Institute, EEI and NEMA have discussed this on the shared cyber security principles back in 2012. As you've heard from my colleagues, supply chain disruption and compromise is a major concern for the electric industry. The EEI and its

member companies recognize that addressing this concern would require collaboration with NEMA and electrical manufacturers, the companies that supply products and services to those utilities. There was a consensus between EEI and NEMA that if we work together to manage supply chain and security risk. NEMA was a partner in this process last year and took a step further in developing this organization NEMA worked to identify guidelines that electrical equipment manufacturers can implement during development and minimize the possibility that bugs, malware, viruses, or other exports can be used to negatively impact operation. In June of last year we published an administrative-incentive white paper on cyber security supply chain best practices manufacturers, otherwise again as CPSP1, supply chain best practices. That is available online at NEMA.org, supply chain best practices. The document's been very well received by manufacturers, utilities, policymakers, and the general public. The document address supply chain integrity through four phases of the product life cycle: First, manufacturing, an analysis during manufacturing to detect and eliminate anomalies in the embedded components of hardware; second, delivery, tamper-proofing, to ensure the manufactured devices can't be altered from the production line to the operating environment; third, operation, ways

that a manufacturer device enables asset owners to comply with security requirements and necessities of the regulated environment, otherwise known as the security development life cycle; four, end of life, decommissioning or revocation processes to prevent compromise or obsolete as being used as a means to penetrate security networks. As opposed to being an all-inclusive document, it's a representation identified best practices that vendors can implements that deliver, manufacture, and deliver products as part of the supply chain.

I'll cite some few examples from the document itself. The manufacture and assembly phase of the product suggests that manufacturers follow a documented purchasing process that gives preference for ensuring the company for only the original equipment, manufacturers or their authorized suppliers. Manufacturers should also have in place some type of industry-recognized inspection technique to discover counterfeit components before they become physically integrated into the product. In the taper-proofing phase, at minimum manufacturers should be required to use some type of tamper resistance, coating, or seal on all hardware components. In the operating system layer, manufacturers should consider using an OS with minimal kernel features in the application stage. In the final, it increases the integrity of the OS component. In

a security development life cycle, at minimum manufacturers should test their products or devices to validate compliance with the security requirements and necessities of the environment. Depending on an environment, third-party testing may be required. In the decommissioning or revocation phase, at minimum manufacturers should use purging or sanitation techniques to remove sensitive data from a system or storage device with the intent that the purged data can't be reconstructed by any known technique.

NEMA and NEMA companies recognize that supply chain cyber security risks are constantly evolving. We want to thank FERC for hosting this very important conference. However, we would like to emphasize that if the market determines the need for additional supply chain standards, they should be voluntary, and the process whereby they're developed should be open and industry-consensus based. NEMA looks forward to working with and being a resource for FERC, NERC, utility and other stakeholders in addressing supply chain issues and risks within the energy sector.

Thank you.

MR. BARDEE: Thank you.

Our next speaker is Maria Jenks from Kansas City Power & Light.

MS. JENKS: Good afternoon. It's a pressure and an honor to be here this afternoon. Like you said, I'm Maria Jenks. I'm the vice president of supply chain for Kansas City Power & Light, also known as KCP&L. By way of background, I spent the last six years in supply chain. Prior to that I led our internal audit function. So I have an understanding of risk management principles.

Like I said, I'm here representing KCP&L. We serve 830,000 customers for residential, commercial, industrial in the western part of Missouri and eastern part of Kansas. We have about 6,600 megawatts of base load generation. We appreciates the Commission's continuing strong interest in critical infrastructure protection supply chain risk management issues, and welcome the opportunity to participate in today's technical conference.

The CIP Version 5 requirements provide the right approach in mandating the what, but not the how, in terms of cyber security in supply chain risk management. KCP&L using existing supply chain risk managements guidelines and practices to help determine the how for regulatory compliance, as well as enterprise-wide risk management. We do not believe a new or modified FERC mandate standard is needed to address the supply chain cyber security risk for industrial control, hard, software, and computing network services associated with bulk electric system operations.

Long-held, fundamental goals for every utility supply chains, whether acquiring turbines, transformers, or cyber assets, is ensuring security and has competence in all of the purchase power services. In light of these fundamental goals, it is simply good business practice to promote supply chain security. As somebody has every incentive to safeguard KCP&L's operational integrity, my comments will summarize KCP&L's current supply chain risk management efforts which are representative of existing utility procurement practices and industrial supply chain initiatives regarding information in technology and hardware/software services also critical to infrastructure sectors.

Supply chain and supply chain risk is not just managed by me and my team. Supply chain is really the nerve center of the utility and cuts across our whole company. So we all work together to help ensure resilient supply chain. We manage supply chain risks through a very collaborative approach, both through our internal stakeholders as well as our suppliers, using widely-accepted standards and frameworks and processes to assess, to manage, and then to monitor those critical risk areas. KCP&L employs and enterprises this management framework based upon a COSO enterprise integrated risk management framework to assess risk, including but not

limited to cyber and physical security, reliability, operational, and supply chain risk, among many other business risks.

Enterprise risk mitigation strategies are supported and then monitored. The process is coordinated by KCP&L's internal risk management department, it engages leaders of businesses across the company. And then on the back end there's added monitoring that happens, not only from risk management but also internal audit, our focus compliance department, our FERC compliance department, and additional assurances through the quality control procedures with the operating units. Basically, enterprise risk is organic and it's foundational throughout the organization, including the supply chain function. So it starts at the enterprise level and cascades down through the departments.

From the supply chain perspective, of offices require the supply chain risk assessments, cyber and physical security risks is a dimension of the assessments and always considered. We also have a supplier risk assessment framework, and we use that to identify and assess suppliers that pose a particular threat, risk or threat, to operations. And we tier that risk, we categorize them based on high, medium, or low priority -- or risk level. Traditionally, supply chain risk assessment

risk is at the front end of the process for every major procurement of goods or services as well. So while the processes and procedures require cyber security, physical security, and reliability risk assessments, they're only a component of the broader range of business risks that are evaluated and mitigated by supply chain.

Once a procurement project is started, purchasing procedures require supply chain work which is often with technical experts throughout the company often involving engineering and the project managers, leveraging their expertise and establishing technical specifications that are included in our request for proposal, or RMP. The RMP provides detailed design to ensure specifications, as well as other technical and standards. The RMP technical specification helps out discussions with prospective suppliers and are critical to the robust evaluation process, including identifying cyber and physical security risks. Risk assessments also guide discussions as to contracting approaches and contracting structure.

KCP&L also utilizes the cyber security procurement language for energy delivery systems that we've heard so much about today, endorsed and promoted by the Department of Energy and the Department of Homeland Security. KCP&L has developed a guideline based on that procurement language to assess risk relating to hardware,

software, and communication-type purchases. Using the guideline, appropriate contract provisions are incorporated into our procurement agreement. And there's been some discussion about these contracts, and the thing that I just wanted to add on to that is: What I have seen is the value of the procurement language is not in the language in and of itself. Because if you rely only on that then you are missing a whole component of the rest. I have seen more value not come out of attorneys battling over specific words within that language, but rather the discussions that those have brought about by having the engineers and the project managers on our side sitting with their counterparts on the supplier side and really talking about the language is trying to mitigate in the particular project and coming to solutions that are beneficial for both sides.

KCP&L also employs a rigorous supplier evaluation process, qualification and approval. And this is prior to contract award. Our due diligence includes items such as safety reference, financial and credit standing, security standards and certifications, other quality and security checks depending on the nature of the work and the risk of the supplier. KCP&L works extensively with suppliers with the understanding of their manufacturing processes, subcontracting plants, supply

chain, and other relevant information relevant to the procurement transaction. Sometimes again we'll perform site visits and inspections if appropriate. We identify whether data is going to be shared amongst the companies, whether the supplier system will interface with our system, and a whole host of other information.

We recognize how difficult it is, and impossible really, to achieve a hundred percent security, but that's why we partner with the federal government. We further assess cyber-aspect risk based on what is received such as the Federal Bureau of Investigation, the Department of Homeland Security, the Electric Information sharing and Analysis Center, and other utilities. We employ a rigorous formal internal review and approval process for each procurement before contracts are signed. We include subject matter experts from risk management, information security, information technology, our corporate security, engineering, operations, warrantee, legal compliance, or other affected stakeholders that review pertinent sections of the contracts prior to execution. Cyber security procurements have subject matter experts for each technical area as well. Controls and protocols are in place to help ensure that the risks identified during the assessment process has an appropriate risk mitigation plan in place with documentation and confirmation at completion.

Then there's the post-contract execution. After a contract is executed, there a number of monitoring activities that occur. Depending on the identified risk level established during the initial risk assessment and based on the nature of the project, KCP&L may require a number of different things such as overseeing the manufacturing process, detailed receipt of inspection, quality control, testing, independent third-party audits or reviews, et cetera. Contract management processes are used to confirm and document execution of developments of the contract, including security-related provisions.

Then we work with our suppliers on an ongoing basis to monitor how the project is going. We work with each supplier that include metrics to regularly track and monitor service-level agreements and policy deliverables. We conduct regular business to report our results and drive reliability, effectiveness, and accountability. KCP&L's change order control process and other contract management processes work to ensure safety plans, security risks, and quality certifications are available and up to date. Ultimately, KCP&L believes setting the right tone and communication to the suppliers is a critical component of its supply chain risk management strategy; it truly is a partnership.

In closing, KCP&L supports EEI's work on

principles and resources and recommendations for managing supply chain cyber security risk. We believe industry participants are responsible for the reliable operation of the bulk electric system will adopt the guidelines and build a system of risk management and control in accordance with the guidelines. In the event there is a need to amend the guidelines, we concur with a number of things that were said here today that collaboration with a broad range of stakeholders is absolutely critical. Not only subject matter experts, having the right legal contract people involved, supply chain experts, information security experts, but also all these stakeholders, utilities, suppliers, government agencies, trade associations like EEI, NEMA, UTC, and others.

And then we also want to encourage an across-industry approach. Many of our suppliers supply not only to the electric utility industry, but they supply to other critical infrastructure areas as well. So I think taking an across-industry approach makes a whole lot of sense. We talked a bunch about a task force today, and I would encourage that as a way to explore and understand and leverage other voluntary guidelines that are available such as the NIST and standards, the DOE procurement language, what NEMA has put out and others, way to share best practices, but to keep it voluntary and flexible as well.

Thank you.

MR. BARDEE: Thank you, Maria.

Our next speaker is Robert McClanahan from the Arkansas Electric Coop Corporation.

MR. McCLANAHAN: Thank you. My name is Robert McClanahan. I'm vice president and chief information officer at Arkansas Electric Coop Corporation. AECC is an electric generation and transmission cooperative in Arkansas that provides wholesale electricity to 17 electric distribution cooperative member owners. These distribution cooperatives in turn provide electric service to approximately 500,000 retail members primarily in Arkansas covering just over 60 percent of the state's geographic area. I would like to thank the Commission staff and Commissioner Honorable for the opportunity to provide testimony this afternoon concerning the important issue of supply chain risk management. I would also like to echo AECC's support of the joint filing by the industry trades in this docket to the effect that a new reliability standard on supply chain is not necessary, nor would it add value in this area.

AECC believes that the risk associated with the supply chain should be analyzed from two broad perspectives: Pre-implementation and post-implementation. We believe that the post-implementation perspective, i.e.,

those rich to a system under our operational control, is beyond the scope of today's proceeding and is sufficiently being addressed through the company-specific cyber security programs based on existing NERC CIP standards. Our program's internal controls appropriately mitigate supply chain risks such as tampering, theft, unauthorized access, and malicious software insertion. The pre-implementation perspective, which includes risk such as manufacturing software development practices and counterfeit hardware and software is far more difficult to control. AECC believes that this difficulty is a direct result of three primary factors: First, utilities the size of AECC do not have a large enough financial impact on vendors to control contractual firms relating to supply chain risk management. As a result we are often left in a position of accepting "take it or leave it" contract terms with little or no ability to negotiate standard contractual provisions, much less pre-implementation supply chain risk controls. Even looking at the electric industry as a whole, AECC believes there is insufficient purchasing power for full control over the contractual terms of procurement. Second, there are numerous supporting information and communication technology, or ICT, assets from multiple vendors that work together to make our control systems function. These include servers, networking equipment storage, and virtual

infrastructure and access control in a monitoring system. Even with proper supply chain risk management for power control systems, any risk assessment of the actual supply chain must factor in the supporting ICT asset. However, has discussed previously, utilities such as at AECC are often in no position to negotiate the contractual terms governing their procurement.

Lastly, vendors are not required to, nor do utilities the size of AECC have the means to, access, assess, or audit supply chain vendors. The only tools available to utilities in this arena are assurances that a vendor provides through third-party assessments and certifications. However, these are often inconsistent in the controls that are tested and do not provide full assurance in the activities conducted during procurement. Because of these three difficulties, as well as the regulation currently in place with NERC CIP, AECC encourages the Commission staff to look toward non-punitive initiatives that encourage wider use of vendor certification, along with research to technologies to assist in the detecting and preventing fraudulent hardware and software. AECC asserts that the industry resource investment would be significantly more effective in these activities rather than in new compliance initiatives.

In conclusion, AECC recognizes that managing

supply chain risk is a vital part of any cyber security program and appreciates the Commission staff highlighting the importance of this issue. This is a challenge that needs additional near-term research and testing. We have confidence that FERC and the industry will continue working together to support effective initiatives and addressing cyber security risk in the supply chain.

Thank you.

MR. BARDEE: Thank you, Robert.

And our final speaker is Thomas O'Brien from PJM. Tom?

MR. O'BRIEN: My name is Tom O'Brien and I am the vice president and chief information officer at PJM Interconnection. I'd like to thank the entire FERC organization for pulling together this serious dialogue in the serious conversation we've been having.

Regardless of the outcome today, this is a good day. It's a good day to create dialogue around potential solutions; we don't have all of the answers. My view on the cyber security supply chain risk is it's critically important. There is evidence of embedded vulnerabilities, embedded attacks. We've seen them, some of them are not but it's a real serious issue. But the positive thing for me in this meeting today is that I saw more commonality than I did difference. And I think that's a great starting

point.

I will let my written comments speak to the details of the PJM point, but I wanted to cover a couple of things. One is I want to talk a little bit about the unique challenges, which was something the panelists were asked about. And I think the unique challenges will really go to answering the question the Commissioner Clark had this morning about what's different around supply chain. I'll talk a little bit about PJM, what we are doing, some of the things around best practices. It won't be comprehensive because I know that time is limited. And finally I would like to talk about a recommendation going forward that I think will help us advance all of this.

Going to the unique challenges, you've heard today that the supply chain, the scope is huge, it's highly distributed, and it does not fall under a single regulatory jurisdiction. That makes it a challenge that makes it different than a lot of things we've had to deal with. The other thing I think is important and is a challenge that the hardware, software, and service vendors, they will not be successful if they are trying to operate to multiple regulatory standards. I think there is some harmonization that needs to occur with those standards, and without that I think we'll be in trouble. The other thing I think you need to be careful of in the standards process or guidance

process of wherever we end up, is that we don't lull ourselves into a false sense of security and we don't divert attention to the things that are most important. And today many of the panelists talked about risk-based approaches, and I think that makes a lot of sense. The other thing -- and this was mentioned by some of the other panelists -- the increased utility cost, we have to be cognizant of that. There's no question that security controls add cost and they are necessary and they must add cost but we need to make sure it's effective and it's efficient with what we're doing. So that kind of summarizes the question I think, again, Commissioner Clark had, what makes supply chain different and unique?

When I look at PJM in the way we operate is for a number of years we've had what we call a security and compliance program, risk-based program, where we're looking at everything we're doing in compliance and security and doing our best to stack up the risks and address things in an incremental fashion based on what we believe is the highest level. As you know, the risk essentially looks as threat, it looks at likelihood, it looks at impact, and we're trying to spend most efficiently the dollars we have to driving the most important things. And the outcome here I think needs to get us to the same place. Some of the things we need to do -- and I won't go into great detail

about this -- but many of the other companies in their analysis of threats, we have people attending classified briefings, we're getting feedback from our government contractors, we're getting feedback from our vendors in terms of what are the threats, we're evaluating those, doing the best we can so that we understand what the threats are. It's not part of a standard right now but it's part of a best practice and something we've been doing.

Others on this panel have mentioned things like vendor review processes. We do that, we look at our vendors, we evaluate based on criticality what kind of controls do they have both cyber and physical. We look at our vendors of high-risk systems, and that probably falls more into the EMS in that domain, we do audits of their site, we spend time with their site, we look at the practices of their domain in terms of managing their environment, our development environments, how are they managing those. And that's a big part of what we do. Something that's ongoing right now, this is something that PJM is doing -- and I give a lot of credit to the other ISO's because it's been a collaborative effort -- putting together common security requirements that can become part of the procurement process and working together on that so that we can drive vendors in a similar direction in our

contracts.

Others mention things like the background screening process. We do the background screening processes. We go beyond typical background screening from the standpoint of everybody that's coming into the critical access area, building as a contractor, all those kind of things. Another key component that I believe is part of supply chain management is active monitoring. There's not a single person that e can fire that can handle supply chain risk. But we look at things like 24 by 7 security monitoring at the security operations center, advanced tools that are looking at what happened to things that are exiting your system. I give a lot of credit to NERC and others around the CRISP, that's the Cyber Risk Information Sharing Program. We know that our network that's actually there's monitoring going on, is there stuff going out to the bad guys? And that's really valuable. I don't think there's a standard on that, but it's certainly a best practice.

So I think I'll shift a little bit more to the recommendation that I believe could be meaningful. And in light of the complexity of everything that's going on, the disparity standards, you've heard today probably more alphabet soup than you've heard between ISO members and I don't mean to minimize that because there's been a lot of

really, really good work done on that. Our recommendation is to find a way to harmonize that. Things like -- and so some of the other panelists, they talk about the NIST cyber security framework, they talk about ISO standards. DOE cyber security procurement language, we have a lot of documents and we have a lot of guidance. The recommendation that I would make would be that FERC direct NERC not to develop a standard but to develop guidance, and that guidance should include -- and I compliment the non-industry folks, Edna Conway, your willingness to volunteer Cisco leadership. But could FERC direct NERC to put together an entire task force -- I'm not sure what we'd call it -- but put together a group that is essentially going to look at this problem from a risk-based perspective and have an outcome that the first delivery is one of the top five supply chain cyber security issues that we would resolve. And then we can start working those, and we're not waiting for a protracted standards process from two years to three years to do it. Because the people in this room have energy around doing this. So if we could do it through a set of guidelines as opposed to a standards process.

The other thing that's critically important, I think this is certainly an area that FERC can help, we've made tremendous progress in the industry around

communications and managements ideas, I give the Electric Sector Coordinating Counsel a lot of credit for that. But I see the ISAC being much more responsive, much more information sharing going back and forth. The thing we're missing is information sharing across all critical infrastructures. So how could this recommendation, where we're looking at risk, how could we be pulling together information? What is the financial sector seeing? What is the telecommunication sector seeing? I think there's a huge opportunity for that kind of collaboration.

In closing, I believe the fastest, most-cost-effective and most value will be driven through this collaborative process across critical infrastructures, across government industries, and across the vendors. We won't get everybody on board initially, but if we can get a subset of that to move the industry and move the critical infrastructures together rather than individually, I think that is our best chance of success.

And with that, I thank you for the opportunity to speak. Thank you.

MR. BARDEE: Thank you, Tom. And thanks to all of our panelists this afternoon.

COMMISSIONER HONORABLE: Good afternoon. I just quickly wanted to thank you. Thank everyone who's still in the room, you get the gold stars. This portion of the

panel, I wanted to try to -- some of my meetings ran longer than I anticipated. But I'm delighted to be back to here, half of at least of the presentations, because this was a very practical, informing session to us about what's happening in the real world, what are you really doing. And that aids us in our evaluation of whether or not we need this in the first place.

Mr. O'Brien, it's clear that there's been some development of thought, probably not embraced by all, about a task force or committee that NERC might be directing. Would that task force or committee, or whatever, other group it might be called -- and I realize this is off the cuff -- would it aid in developing this guidance? Or who's on first?

MR. O'BRIEN: I would see it as aiding in the guidance. And I think based on this recommendation it's essentially asking FERC to direct NERC to lead it. I do recognize that there is a lot of other things going on. DOE is doing things, there's a bunch of people doing things. I think to the extent we can get people together and people want to do it as a team as opposed to disparity efforts, I think it gives us the best chance. And a deliberate coming-out of it would be what if the Committee came out within X months -- I don't want to put a timeline on it -- the top five risks that we should be building best

practices around, and we're sharing that information, we're working with the vendors, we're learning from them, they're learning from us, across all those infrastructures, I think that would be huge and I think it's a huge opportunity for us.

COMMISSIONER HONORABLE: To follow that, then allowing that discussion to guide the guidance that would hopefully serve to harmonize all of these different sources of information?

MR. O'BRIEN: Yes, that's exactly right. The intent would be to harmonize all of the information that out there. I've learned more in the last couple months by talking to our vendors, understanding physical supply chain, understanding chains of custody, there's a lot of good information out there. And unfortunately, as I said earlier, we don't have control over all of that as the end customer, but we have learned about it. And somebody made a comment earlier today that if we could point the vendors in the right direction, whether it be a standard or a guidance, the market will drive behavior. And we're all asking the similar question. We're going to chose the vendors that enforce best practices around cyber security because it's that important.

MR. BARDEE: Mr. Bochman, I had a question for you. I saw that not long ago you had on simplicity in

energy infrastructure. I wondered if you could sort of describe the basic theme of your paper and whether what you suggested there would help address any of the risks that have been discussed here today?

MR. BOCHMAN: I'll keep this real short to allow time for further questions and answers. The paper is called Case for Complexity in Energy Infrastructure published by CSI think tank. Basically contends that in addition to all of the complexity that we've been learning about today, the supply chain and their incumbent security risk that comes with them, that the overwhelming technical complexity of many of UST utilities most-essential energy generation transmission distribution processes makes our cyber adversary's jobs much easier than they should be. It suggests selectively reducing complexity by, among other things, putting a trusted man back in the loop, he or she was removed for efficiency reasons; inserting analogue at those service disruption boards in the immediate pathway to the cyber physical target; and other out-of-band solutions. Often this will mean the removal of unnecessarily complex general systems that support these processes today. And in so doing, this may serve to simplify and reduce certain utility supply chain vulnerabilities and dependencies. Mind you, if you read the paper, it's very emphatic that this is not a broad recommendation for a great deal of

utility systems but only for the holiest of holy, the things that must never be brought down by cyber means.

MR. BARDEE: Thank you.

Mr. Whitehead, given your line of business, do you have any thoughts on that?

MR. WHITEHEAD: About the Holy Grail?

(Laughter).

MR. BARDEE: No.

MR. WHITEHEAD: But I think I could echo probably on the theme. We've always taken an approach, and I think many people have said there is not going to be one overall that mitigates all of our supply chain challenges. As we said, it's a global economy, we get parts from all over the place. Certainly, from a manufacturer standpoint, you can count on us to make sure we know how we manage all that stuff. We ultimately provide a reliable product to our customer. It's not just one product. We've used the word "security" in depth. And I think that's really a reason to that effect going back to when we were talking about risk mitigation and how a system is designed if we have an M minus 1 failure what we need in the system. So all of those, taking that approach at our company, we're designing systems for our customers about if the devices become compromised or fail just because there's a memory problem, it's out of service, how does the rest of the

service respond? I think that kind of echoes with there is no Holy Grail, there can only be a security in-depth approach.

MR. BARDEE: Mr. Ginter, I had a question for you. Earlier today there was some discussion about vendor access in the sense of not only being able to receive data but also bidirectionally being able to send commands or change settings remotely. I understand the products you offer would be unit-directional in allowing the receiving of the data but not the direct removal/control of any devices. But other witnesses today were saying that some of the controls under CIP Version 5 -- at least if I understood their premise right -- your technology might not be necessary or as critical to them. And I wondered what you've been hearing lately in your discussions with potential customers or what your thoughts are on CIP Version 5 and whether it reduces the value of a unit-directional approach?

MR. GINTER: We were actually very happy that CIP Version 5 recognized the technology in the definition of external-level connectivity. So I would say, if anything, the standards have served to increase the visibility of this alternative to firewalls. In terms of remote controls, yes, the flagship product, the initial gateway can only go one way; nothing gets back, remote

control is impossible. This is what we want most of the time with most of our cloud vendors. I've described a couple of technologies when occasional control is needed, occasional remote access. We are seeing electric utilities deploying this technology in an even-wider variety of circumstances.

Very briefly, there's software involved as well. The hardware allows the security of copies of servers. So the software, unlike the firewall, never forwards messages; it makes copies of servers. So we are seeing utilities deploy this technology, making one set of copies of servers outbound and a different set of copies of servers inbound. So a message path that can be used as an attack path, it is copying servers. And when continuing remote control is obviously essential, there are still solutions that are stronger than firewalls for those circumstances as well. I don't know if that's what you were asking, though.

MR. BARDEE: I think that's helpful, though. That does answer my question.

MS. DUNFEE: We've talked about cost a lot and the cost of the standards. But I thought that Mr. Bauder and Ms. Jenks, you talked about a lot of work that you've done in implementing your supply chain risk programs that they seem very comprehensive. If you could talk a little bit about costs of that or has it greatly added to the

cost? And then for Mr. Bauder, perspective from the other side, the program that you all have put together, have you talked about those costs?

MR. BAUDER: Maybe a little bit about the risk programs themselves. When we implement the enterprise risk program we take a point of view that risk is probability times consequence, and then we build a matrix. So it doesn't matter what we're looking at: We could be looking at cyber risk; or we could be looking at, in my case, vendors doing vegetation management in Southern California the risk can be very high. We can have a very costly wildfires or can even take out transmission services; that's happened. So when I qualify those vendors using the score card approach, we look at what are the contractual terms; we look at their insurance requirements; we look at their past record; and we look at their controls and we sample their field activity. So we get very much into their business. That partnership is the same if you're in the cyber world and you're trying to qualify a vendor to do delicate cyber work. There is some incremental costs, yes, but when you look at the risks per and you're eliminating this big event which can really cause harm, and it doesn't matter if it's in the cyber area or in some other area.

MS. JENKS: I would agree with that. We have devoted a significant amount of resources in implementing

an enterprise initiative program. But we also see it as protecting the overall enterprise from bigger consequences that could occur, right. And that cascades down into the organization. So I don't think I have much more to add.

MR. GRIFFITH: Obviously cost is a concern because when you're trying security things, it's going to cost more. I think that comes to the part that market is going to dictate to move toward more and more of these products. So you're going to be seeing -- and I think we're already seeing this -- a lot of these contract are requiring these be built in. So obviously in order to compete members are going to have to level their playing field.

MR. PHILLIPS: Mr. O'Brien, Ms. Jenks, and Mr. Bauder, from a registered entity perspective, I was just wondering if you could speak to the types of disclosures that your organizations will typically seek to require from your vendors whenever you're developing and implanting a new system?

MR BAUDER: Are we talking about cyber disclosures?

MR. PHILLIPS: Yeah, just from a security perspective, what types of things do you look at and what information before you make a decision?

MR. BAUDER: So we'll look for things like what

level of cyber events the vendor has had. Have they had any issues with malware? Have they had any issues with inappropriate control software? Issue with intellectual property? If we think there's going to be a problem there, we'll actually negotiate with who owns and controls the intellectual property. Once again, it's a negotiation back-and-forth, though. We do run into situations with vendors having an ongoing matter that is obviously protected under legal privilege. We respect that; we're not going to demand the recording of that event in that particular case.

MR. PHILLIPS: I think just to elaborate a little bit further: Would you look at things like ask them to disclose if they have hard-coded passwords and things like that in the product that you might want to be aware of from a risk perspective before you put that device or software into service?

MR. BAUDER: I missed what you said about passwords.

MR. PHILLIPS: So would you seek a disclosure on hard-coded passwords, things of that nature, before you would actually decide to put a device into service?

MR. BAUDER: We would expect a vendor to let us know about something like that, yes. Obviously, if you have a problem, something like a backdoor to a software

platform, that's something we would want to have disclosed as well. There's various aspects of IT disclosures that we would demand. Part of that relationship with the vendor, though, to have that dialogue with us, we're interested in past issues and what the vendor has done to close those issues and prevent reoccurrence.

MS. JENKS: Also, similar to Doug, we also look at past incidents and we'll dig into that extensively. In addition to that, we might ask for copies if they've had any third-party assessments or audits done, we might ask for copies of that. If they do have any certifications, we will ask for that. We will talk to them a whole lot about their protocols for information and data-sharing, such as their encryption techniques and that type of thing. We will talk to them about their subcontracting claim and making sure that we understand if they're going to subcontract any of the work or if they're going to do it themselves. And if they're going to subcontract, is any of that going to be done offshore. And we've got very strict requirements around anything like that. We also talk to them about the screening and the background checks that they do for their own internal employees that might be working on our project. And then finally we'll talk to them about their general quality assurance quality control programs and understand what those are, what those involve.

MR. BOCHMAN: Just briefly, as the gentleman from Arkansas said on the panel, the ability to significantly effect the ability of a large software company decreases with the size of your entity. And you can have -- and conversely if you're dealing with a start-up or a smaller software company or services company, you can get a lot from them that you wouldn't get from the larger companies. And I'd say even when we're aggregated as NERC our ability to significantly change the behavior exposure of supply chain from the largest of the large software companies is going to be modest at best, and to keep that in mind as we're thinking about what we're going to do.

MR. O'BRIEN: I would just add a couple of things. One of my colleagues said it depends on the size of the project. Something like an energy management system is we do develop a comprehensive set of requirements; we share with the vendor; and that's something that we test against those to make sure they're doing things. That includes things like how they integrate into our architecture, how they authenticate their systems, things like all password management, all passwords, they're allowed to have known passwords that are stored away somewhere, and we do a lot with that. But the other thing we do in addition that I think is pretty effective is,

again, for our major projects new applications going into production is we work with a niche consulting firm that actually does penetration and is not an internal audit penetration, it's very transparent. And they try to break it. They go in and they look at things and they do an assessment. And if there's defects we put them into the production environment, we go back to the vendor and have them look at those defects. So we work pretty closely with them.

The other thing is that the vendors, there's tools that can do applications scanning looking for vulnerabilities. There's a lot of information in there, that's one of the advances that we're looking at, how they work with vendors.

MR. PHILLIPS: Are the things that you do in negotiating with the contract to say, you know, you're requesting this level of access, I'm not sure you need that access to my system, are there ways you can influence that in the contracting process or other processes to say, you know, we would like greater control over our system for this particular service that we're looking to have somebody provide?

MR. O'BRIEN: Absolutely. For the most part any type of vendor access is closed unless there's a critical reason it needs to be open. So we don't have our RENS

system open for people to walk into and do things to. And that is in the contract. The other thing that's important is we work together on those requirements because it isn't -- they have good ideas too in terms of what they're doing with other customers. But it's a very transparent, open process in terms of what's expected in security perspective. And it's getting better, I had mentioned earlier, the collaboration between the ISO's is really good and we've learned from others from what they're putting in their contracts. We've all committed to growing that and using that in our contracts.

MR. PHILLIPS: I have one just question, just kind of seizing on some of the discussions we've had today on information silos between different organizational units. I just wanted to put out to the panel if there's any sort of management-level controls or things of that nature that would be useful for breaking down those barriers within an organization? So, for instance, putting a CIO or CISO, requiring them to sign off on a major purchase of that nature, if that would be helpful? And that could be in voluntary or mandatory framework.

MS. JENKS: We already do that. So we have a very formal sign-off procedure around all of our procurements. And so if there is something that involves a technical purchase of any sort, or Chief Information

Officer is required to sign off on it, as well as the business or whoever. So it might be legal signing off on it, it might be our CIO, it might be or information officer, depending on the level. So we've got a delegation authority matrix and we have a procedure that dictates which subject matter expert/experts need to physically sign off on a contract before it's executed.

MR. BARDEE: With that, we will end our conference here today. I would like to thank all the speakers on this panel, as well as the earlier panels, and thank our audience for hanging in there for the whole day, it's impressive. So thank you all.

(Whereupon the FERC technical conference scheduled for 11:00 a.m. on January 28th, 2016, was concluded at 5:03 p.m.)